SIGNAMAX™
CONNECTIVITY SYSTEMS

Signamax Connectivity Systems
Model 065-7840
24-Port 10/100/1000BaseT/TX
Managed Switch
U s e r ' s G u i d e

Signamax Connectivity Systems
Model 065-7840

24-Port 10/100/1000BaseT/TX
Managed Switch
U s e r ' s G u i d e

Release 1.0

Release Date: July, 2005

Signamax Connectivity Systems
1810 N.E 144th Street
N. Miami, FL 33181
800-446-3277
www.Signamax.com

Table of Contents

CAUTION ---------- VIII
ELECTRONIC EMISSION NOTICES ---------- VIII

CHAPTER 1. INTRODUCTION ---------- 2

1-1. OVERVIEW OF THE 065-7840 MANAGED SWITCH ---------- 2
1-2. CHECKLIST ---------- 4
1-3. FEATURES ---------- 4
1-4. VIEW OF THE 065-7840 MANAGED SWITCH ---------- 7
1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs) ----- 7
1-4-2. User Interfaces on the Rear Panel ---------- 8
1-5. VIEW OF THE OPTIONAL MODULES ---------- 9

CHAPTER 2. INSTALLATION ---------- 10

2-1. STARTING THE 065-7840 MANAGED SWITCH UP ---------- 10
2-1-1. Hardware and Cable Installation ---------- 10
2-1-2. Cabling Requirements ---------- 11
2-1-2-1. Cabling Requirements for TP Ports ---------- 12
2-1-2-2. Cabling Requirements for 1000SX/LX SFP Module ---------- 12
2-1-2-3. Switch Cascading in Topology ---------- 13
2-1-3. Configuring the Management Agent of the 065-7840 Managed Switch ---------- 16
2-1-3-1. Configuring the Management Agent of the 065-7840 Managed Switch through the Serial RS-232 Port ---------- 17
2-1-3-2. Configuring the Management Agent of the 065-7840 Managed Switch through the Ethernet Port ---------- 19
2-1-4. IP Address Assignment ---------- 20
2-2. TYPICAL APPLICATIONS ---------- 25

CHAPTER 3. OPERATION OF WEB-BASED MANAGEMENT ---------- 27

3-1. WEB MANAGEMENT HOME OVERVIEW ---------- 28
3-1-1. System Information ---------- 31
3-1-2. IP Configuration ---------- 33
3-1-3. Time Configuration ---------- 36
3-1-4. Account Configuration ---------- 39
3-2. PORT CONFIGURATION ---------- 40
3-2-1.Port Status ---------- 40
3-2-2. Port Configuration ---------- 45
3-2-3. Simple Counter ---------- 47
3-2-4. Detail Counter ---------- 49

3-3. MIRROR ---- 52
3-4. BANDWIDTH MANAGEMENT ---- 53
3-5. QOS(QUALITY OF SERVICE) CONFIGURATION ---- 55
3-6. SNMP CONFIGURATION ---- 65
3-7. IGMP SNOOPING ---- 67
3-8. MAX. PACKET LENGTH ---- 69
3-9. DHCP BOOT ---- 70
3-10. VLAN ---- 71
3-10-1. VLAN Mode ---- 71
3-10-2. Tag-based Group ---- 74
3-10-3. Port-based Group ---- 76
3-10-4. Tag Rule ---- 78
3-11. MAC TABLE ---- 80
3-12. GVRP CONFIGURATION ---- 87
3-13. STP CONFIGURATION ---- 93
3-13-1. STP Status ---- 93
3-13-2. STP Configuration ---- 95
3-13-3. STP Port Configuration ---- 97
3-14. TRUNKING CONFIGURATION ---- 100
3-15. 802.1X CONFIGURATION ---- 107
3-16. ALARM CONFIGURATION ---- 117
3-17. CONFIGURATION ---- 120
3-17-1. Save/Restore ---- 121
3-17-2. Config File ---- 123
3-18. DIAGNOSTICS ---- 124
3-19. TFTP SERVER ---- 127
3-20. LOG ---- 128
3-21. FIRMWARE UPGRADE ---- 130
3-22. REBOOT ---- 131
3-23. LOGOUT ---- 132

CHAPTER 4. OPERATION OF CLI MANAGEMENT ---- 133

4-1. CLI MANAGEMENT ---- 133
4-1-1. Login ---- 133
4-2. COMMANDS OF CLI ---- **ERROR! BOOKMARK NOT DEFINED.**
4-2-1. Global Commands of CLI ---- **Error! Bookmark not defined.**
4-2-2. Local Commands of CLI ---- **Error! Bookmark not defined.**

CHAPTER 5. MAINTENANCE ---- 213

5-1. RESOLVING NO LINK CONDITION ---- 213
5-2. Q&A ---- 213

APPENDIX A TECHNICAL SPECIFICATIONS ---- 214

APPENDIX B NULL MODEM CABLE SPECIFICATIONS ---- 217

Revision History

Release	Date	Revision
0.95	04/15/2005	A1
0.95	04/22/2005	A1
0.95	05/11/2005	A1

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

About this user's manual

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the 065-7840 Managed Switch through the built-in CLI and web by RS-232 serial interface and Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface and command-line interface (CLI).

Overview of this user's manual

- Chapter 1 "Introduction" describes the features of the 065-7840 Managed Switch
- Chapter 2 "Installation"
- Chapter 3 "Operation of Web-based Management"
- Chapter 4 "Operation of CLI Management"
- Chapter 5 "Maintenance"

1. Introduction

1-1. Overview of the 065-7840 Managed Switch

The 065-7840 Managed Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast, and standard Ethernet specifications. The switch includes 22-Port 10/100/1000 Mbps TP and 2-Port Gigabit TP/SFP Fiber management Ethernet switch. The switch can be managed through its RS-232 serial port via direct connection, or through an Ethernet port using its Command Line Interface (CLI) or the Web-based management Graphical User Interface (GUI) associated with its SNMP agent. With the SNMP agent, the network administrator can log on to the switch to monitor, configure and control each port's activity in a user-friendly way. The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful functions such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, and IGMP Snooping capability via the intelligent switching software. It is suitable for both metro-LAN and office applications.

In this switch, Ports 23 & 24 includes two types of media --- TP (**T**wisted **P**air) and SFP (**S**mall **F**orm-factor **P**luggable) Fiber (LC, BiDi LC…); this port supports 10/100/1000 Mbps TP or 1000 Mbps SFP Fiber with an auto-detection function. 1000 Mbps SFP Fiber transceiver is used for high-speed connection expansion.

- 1000 Mbps LC, Multimode, SFP Fiber transceiver
- 1000 Mbps LC, singlemode 10 km, SFP Fiber transceiver
- 1000 Mbps LC, singlemode 30 km, SFP Fiber transceiver
- 1000 Mbps LC, singlemode 50 km, SFP Fiber transceiver
- 1000 Mbps BiDi LC, singlemode 20 km, 1550nm SFP Fiber WDM transceiver
- 1000 Mbps BiDi LC, singlemode 20 km, 1310nm SFP Fiber WDM transceiver

Each 10/100/1000 Mbps TP port is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast, and standard Ethernet specifications. 1000 Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000 Mbps Single Fiber WDM (BiDi) transceiver is designed with an optical Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signals over a single fiber simultaneously.

For upgrading firmware, please refer to Section 3-21 or Section 4-2-2 for more details. The switch will not stop operating while upgrading firmware and after that, the configuration remains unchanged.

• Key Features

QoS:

Support Quality of Service by the IEEE 802.1P standard. There are two priority queue and packet transmission schedules using Weighted Round Robin (WRR). User-defined weight classification of packet priority can be based on either a VLAN tag on packet or a user-defined port priority.

Spanning Tree:

Supports IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) and IEEE 802.1s (MSTP: Multiple Spanning Tree Protocol) standards.

VLAN:

Supports Port-based VLAN and IEEE802.1Q Tag VLAN. Supports 256 active VLANs and VLAN ID 1~4094.

Port Trunking:

Support static port trunking and port trunking with IEEE 802.3ad LACP.

Bandwidth Control:

Support ingress and egress per port bandwidth control.

Port Security:

Support allowed, denied forwarding and port security with MAC address.

SNMP/RMON:

SNMP agent and RMON MIB. In the device, the SNMP agent is client software which is operating over SNMP protocol used to receive the command from a SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Additionally, the SNMP agent will actively issue TRAP information when it occurs.

RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, VLAN MIB (802.1Q, RFC2674), Ethernet MIB (RFC 1643) and so on.

IGMP Snooping:

Support IGMP version 2 (RFC 2236): The IGMP snooping function is used to establish the multicast groups to forward the multicast packet to the member ports, and avoid wasting the bandwidth while IP multicast packets are running over the network.

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- The 065-7840 Managed Switch
- Mounting Accessory (for 19” Rack Shelf)
- This User's Manual on CD-ROM
- AC Power Cord
- RS-232 Cable

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

1-3. Features

The 065-7840 Managed Switch, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

• Hardware

- 22 10/100/1000 Mbps Auto-negotiation Gigabit Ethernet TP ports
- 2 10/100/1000 Mbps TP or 1000 Mbps SFP Fiber dual media auto-sensing ports
- 400KB on-chip frame buffer
- Jumbo frame support
- Programmable classifier for QoS (Layer 4/Multimedia)
- 8K MAC address and 4K VLAN support (IEEE802.1Q)
- Per-port shaping, policing, and Broadcast Storm Control
- IEEE802.1Q-in-Q nested VLAN support
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-24: LINK/ACT, 10/100/1000 Mbps, SFP Port 23,24: SFP(LINK/ACT)

• Management

- Supports concise port status information and easy port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system Information when you login
- Supports port mirroring functionality
- Supports static trunking functionality
- Supports 802.1Q VLAN
- Supports user management and limits three users to login
- Maximal packet length can be up to 9216 bytes for jumbo frame application
- Supports DHCP Broadcasting Suppression to avoid network suspensions or crashes
- Supports the sending of trap events while monitored events happen
- Supports default configuration which can be restored to overwrite the current configuration which is working on via web browser and CLI
- Supports on-line plug/unplug of SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- Built-in web-based management and CLI management, providing a more convenient user interface
- Supports port mirroring function with ingress traffic
- Supports rapid spanning tree (802.1w RSTP)
- Supports 802.1x port security on a VLAN
- Supports user management with only the first logged-in administrator able to configure the device. The rest of users can only view the switch.
- SNMP access can be disabled, preventing undesired SNMP access
- Maximal packet length can be up to 9,216 bytes
- Supports Ingress, Non-unicast and Egress Bandwidth rating management with a resolution of 1 Mbps
- The trap event and alarm message can be transferred via e-mail and mobile phone short message
- Supports diagnostics, to let administrator know the hardware status
- Supports external loopback test, to check if the link is ok
- TFTP for firmware upgrade, system log upload and configuration file import/export

- Supports remote boot of the device through user interfaces and SNMP
- Supports network time synchronization and daylight savings time
- Supports 120 event log records in the main memory and display on the local console

1-4. View of the 065-7840 Managed Switch

Fig. 1-1 Full View of the 065-7840 Managed Switch

1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 24 TP Gigabit Ethernet ports and 2 SFP fiber ports for optional removable modules on the front panel of the switch. The LED display area, located on the left side of the panel, contains a Power LED, which indicates the power status and 24 ports working status of the switch.

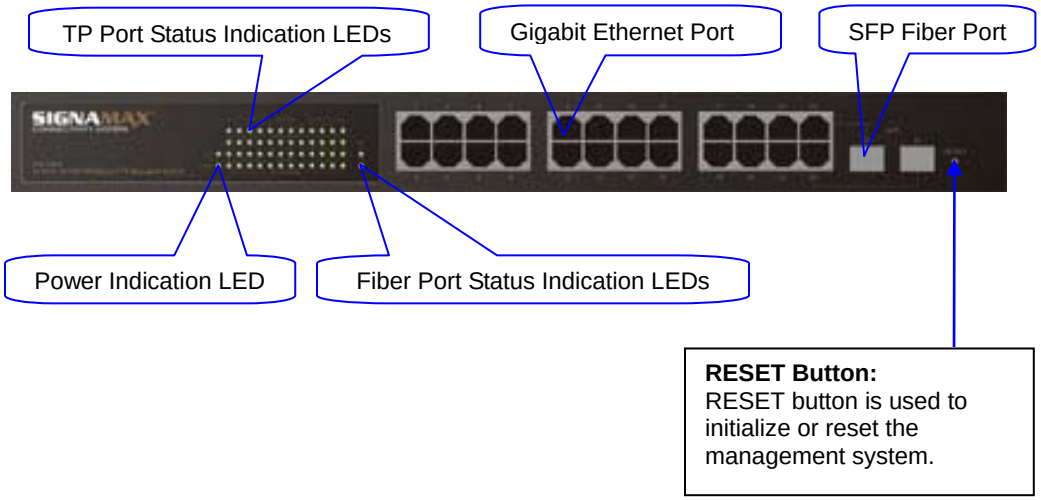

TP Port Status Indication LEDs
Gigabit Ethernet Port
SFP Fiber Port
SIGNAMAX
Power Indication LED
Fiber Port Status Indication LEDs
RESET Button:
RESET button is used to initialize or reset the management system.

Fig. 1-2 Front View of the 065-7840 Managed Switch

• **LED Indicators**

LED	Color	Function
System LED		
POWER	Green	Lit when +5V DC power is on and good
CPU LED	Green	Blinks when CPU is activity
10/100/1000Ethernet TP Port 1 to 24 LED		
LINK/ACT	Green	Lit when connection with remote device is good Blinks when any traffic is present Off when cable connection is not good
10/100/1000 Mbps	Green/ Ember	Lit green when 1000 Mbps speed is active Lit ember when 100Mbps speed is active Off when 10Mbps speed is active
1000SX/LX Gigabit Fiber Port 23, 24 LED		
SFP(LINK/ACT)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Table1-1

1-4-2. User Interfaces on the Rear Panel

One RS-232 DB-9 interface is offered for configuration or management.

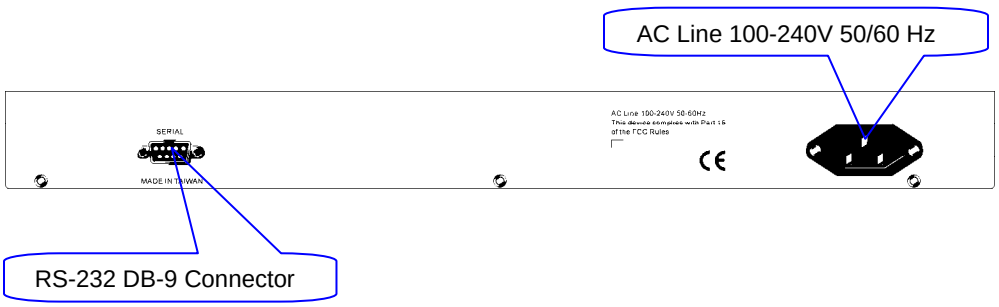


Fig. 1-3 Rear View of the 065-7840 Managed Switch

1-5. View of the Optional Modules

In the switch, Ports 23 & 24 include two types of media --- TP and SFP Fiber (LC, BiDi LC…); this port supports 10/100/1000 Mbps TP or 1000 Mbps SFP Fiber with an auto-detection function. A 1000 Mbps SFP Fiber transceiver is used for high-speed connection expansion; nine optional SFP types provided for the switch are listed below:

- 1000 Mbps LC, MM, SFP Fiber transceiver
- 1000 Mbps LC, SM 10 km, SFP Fiber transceiver
- 1000 Mbps LC, SM 30 km, SFP Fiber transceiver
- 1000 Mbps LC, SM 50 km, SFP Fiber transceiver
- 1000 Mbps BiDi LC, type 1, SM 20 km, SFP Fiber WDM transceiver
- 1000 Mbps BiDi LC, type 2, SM 20 km, SFP Fiber WDM transceiver
- 1000 Mbps LC, SM 10 km, SFP Fiber transceiver with DDM

Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

Fig. 1-5 Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

2. Installation

2-1. Starting the 065-7840 Managed Switch Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

At the beginning, please do first:

⇒ Wear a grounding device to avoid the damage from electrostatic discharge

⇒ Be sure that power switch is OFF before you insert the power cord to power source

• Installing Optional SFP Fiber Transceivers into the 065-7840 Managed Switch

Note: If you have no modules, please skip this section.

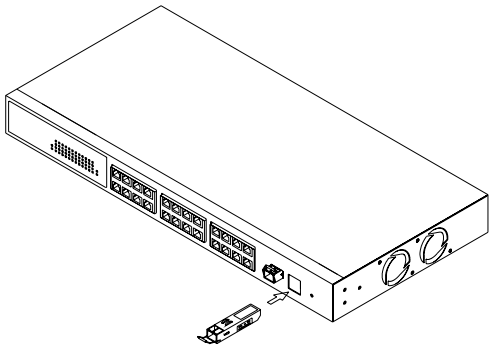


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

• Connecting the SFP Module to the Chassis:

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Turn the power ON after the above procedures are done

- **TP Port and Cable Installation**

⇒ In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. It means you do not have to tell from them, just plug it.

⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.

⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

Now you can begin to operate the switch.

• Power On

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection is plugged into the switch or not when powered on, even the SFP modules as well. After the power is on, all LED indicators will light up immediately and then all will turn off except the power LED, which remains on. This indicates a reset of the system.

• Firmware Loading

After resetting, the boot loader will load the firmware into the memory. It will take about 30 seconds; after that, the switch will flash all the LEDs once, automatically perform a self-test, and is then in a ready state.

2-1-2. Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take care to comply with the cabling requirements. Cables with lower specifications will cause the LAN to operate poorly.

2-1-2-1. Cabling Requirements for TP Ports

⇒ Fast Ethernet TP network connection
- — The grade of the cable must be Cat. 5 or better with a maximum length of 100 meters.

⇒ Gigabit Ethernet TP network connection
- — The grade of the cable must be Cat. 5e or better with a maximum length of 100 meters. Cat. 6 is recommended.

2-1-2-2. Cabling Requirements for 1000SX/LX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multimode (MM) and singlemode (SM). The interface types are categorized into several classes by the types of fiber optic cable used and the distances they support. The 1000Base fiber interface categories are SX, LX, LHX, XD, and ZX. From the viewpoint of connector types supported in the SFP modules used by this switch, there mainly are LC and BIDI LC.

- — Gigabit Fiber with multimode LC SFP module
- — Gigabit Fiber with singlemode LC SFP module
- — Gigabit Fiber with BiDi singlemode LC 1310 nm transmitter SFP module
- — Gigabit Fiber with BiDi singlemode LC 1550 nm transmitter SFP module

The following table lists the types of fiber that Signamax currently supports using SFP modules. Those others not listed here are available as a special order upon request.

<table>
<tr><td rowspan="4">IEEE 802.3z Gigabit Ethernet 1000SX 850nm</td><td colspan="4">Multimode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multimode 62.5/125μm</td><td colspan="2">Multimode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-Km</td><td>220m</td><td>400MHz-Km</td><td>500m</td></tr>
<tr><td></td><td>200MHz-Km</td><td>275m</td><td>500MHz-Km</td><td>550m</td></tr>
<tr><td rowspan="3">1000Base-LX/LHX/XD/ZX</td><td colspan="4">Single-mode Fiber 9/125μm</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310nm 10 km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550nm 30, 50 km</td></tr>
<tr><td rowspan="4">1000Base-LX Single Fiber (BIDI LC)</td><td colspan="2" rowspan="2">Single-Mode *20 km</td><td>TX(Transmit) 1310nm</td><td></td></tr>
<tr><td>RX(Receive) 1550nm</td><td></td></tr>
<tr><td colspan="2" rowspan="2">Single-Mode *20 km</td><td>TX(Transmit) 1550nm</td><td></td></tr>
<tr><td>RX(Receive) 1310nm</td><td></td></tr>
</table>

Table2-1

2-1-2-3. Switch Cascading in Topology

• Takes the Delay Time into Account

Theoretically, a switch partitions the collision domain for each port in switch cascading, so that you may uplink an unlimited number of switches. In practice, the network extension (cascading levels & overall diameter) must follow the constraints of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Converter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01μs (1sec./100 Mega bit)			

Table 2-2

The sum of all elements' bit-time delay and the overall bit-time delay of wires/devices must be within the Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the SFP fiber modules to extend the TP node distance over long distances via fiber optic cabling and provide long haul connections.

• Typical Network Topology in Deployment

A hierarchical network with minimum levels of switching may reduce the timing delay between a server and its client stations. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop, and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. The Server/Host is recommended to be connected to the Level 1 switch. This is general practice, if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-2).

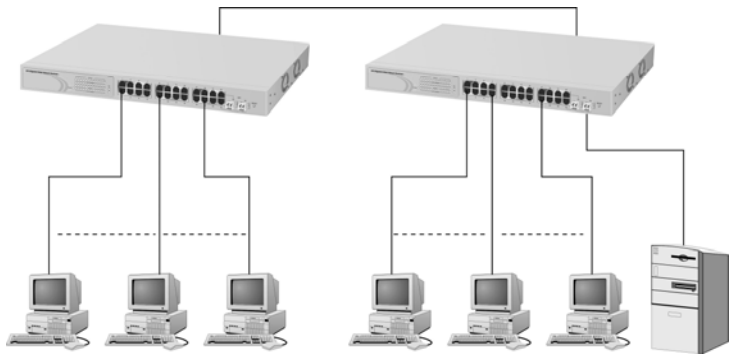


Fig. 2-2 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here the VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagrams show how they work and what the differences between them are:

Case2a: Port-based VLAN (See Fig.2-3).

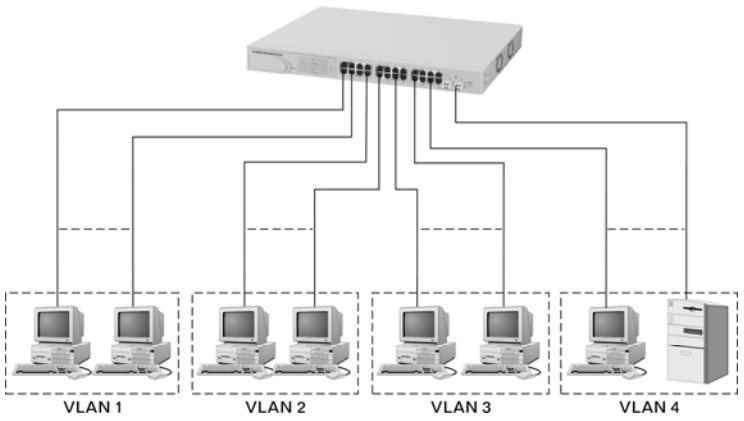


Fig. 2-3 Port-based VLAN Diagram

1. The same VLAN members could not be in different switches.
2. Every VLAN members could not access VLAN members each other.
3. The switch manager has to assign different names for each VLAN groups at one switch.

Case 2b: Port-based VLAN (See Fig.2-4).

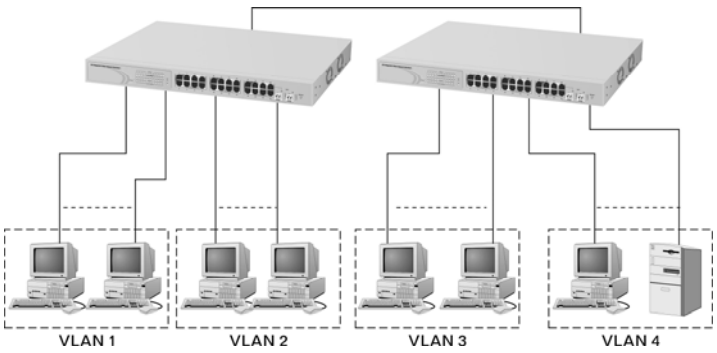


Fig. 2-4 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-5).

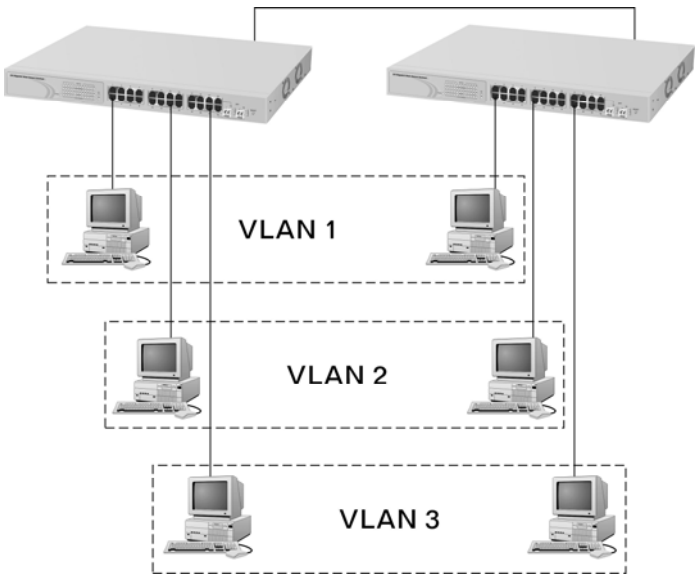


Fig. 2-5 Attribute-based VLAN Diagram

2-1-3. Configuring the Management Agent of the 065-7840 Managed Switch

The Signamax 065-7840 switch offers you three ways to start up the switch management function. They are: RS-232 local console; CLI; and the Web-based GUI. Users can use any one of them to monitor and configure the switch. You can work with them using the following procedures:

Section 2-1-3-1: Configuring the Management Agent of the 065-7840 Managed Switch through the Serial RS-232 Port

Section 2-1-3-2: Configuring the Management Agent of the 065-7840 Managed Switch through the Ethernet Port

Note: First, please modify the IP address, Subnet mask, Default gateway and DNS using the RS-232 console, and then use the desired user interface.

2-1-3-1. Configuring the Management Agent of the 065-7840 Managed Switch through the Serial RS-232 Port

To perform the configuration through the RS-232 console port, the switch's serial port must be directly connected to a DCE device -- for example, a PC -- through an RS-232 cable with a DB-9 connector. Next, run a terminal emulator with the default setting of the switch's serial port. With this, you can communicate with the switch.

In the switch, the RS-232 interface only supports a data rate of 57.6 kbps with 8 data bits, 1 stop bit, no parity check and no flow control.

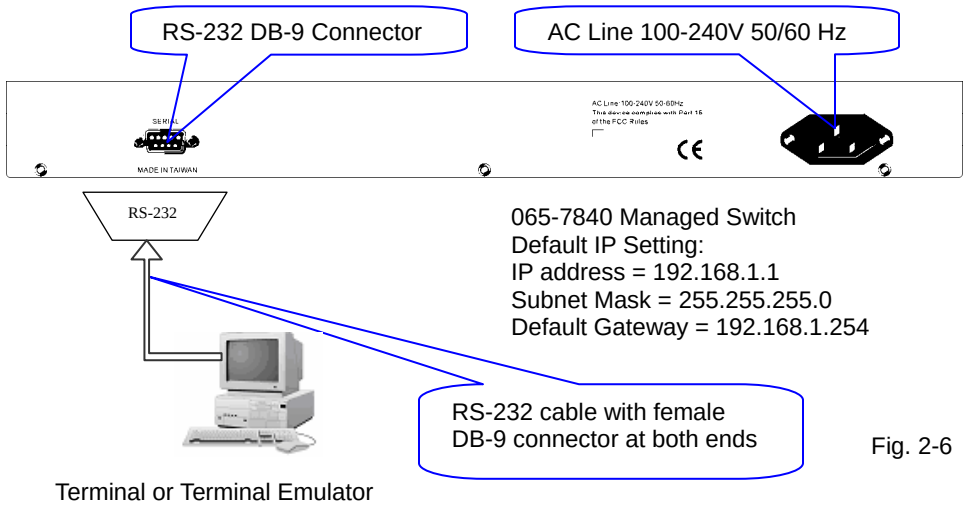


Fig. 2-6

To configure the switch, please follow the procedures below:

1. Find the RS-232 DB-9 cable with female DB-9 connector bundled with the switch. Normally, it just uses pins 2, 3 and 7. See also Appendix B for more details on Null Modem Cable Specifications.
2. Attach the DB-9 female cable connector to the male serial RS-232 DB-9 connector on the switch.
3. Attach the other end of the serial RS-232 DB-9 cable to the PC's serial port, running a terminal emulator supporting VT100/ANSI terminal with the switch's serial port default settings. (For example, Windows98/2000/XP HyperTerminal utility.)

Note: The switch's serial port default settings are listed as follows:

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4. When you complete the connection, then press **<Enter>** key. The login prompt will be shown on the screen. The default username and password are shown as below:

Username = admin Password = admin

• Set IP Address, Subnet Mask and Default Gateway IP Address

Please refer to Fig. 2-6, Console Management, for details about the factory settings. This is the default setting of the switch's IP address. You can first either configure your PC's IP address or change the IP address of the switch, and then change the IP address of the default gateway and the subnet mask.

For example, your network address is 10.1.1.0, and subnet mask is 255.255.255.0. You can change the switch's default IP address 192.168.1.1 to 10.1.1.1 and set the subnet mask to be 255.255.255.0. Then, choose your default gateway, for example, set it to 10.1.1.254.

Default Value	the 065-7840 Managed Switch	Your Network Setting
IP Address	192.168.1.1	10.1.1.1
Subnet	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.254	10.1.1.254

Table 2-3

After completing these settings in the switch, you must reboot the switch to have the new configuration take effect. After this step, you can operate the switch's management functions through the network, no matter if it is from a web browser or a Network Management System (NMS).

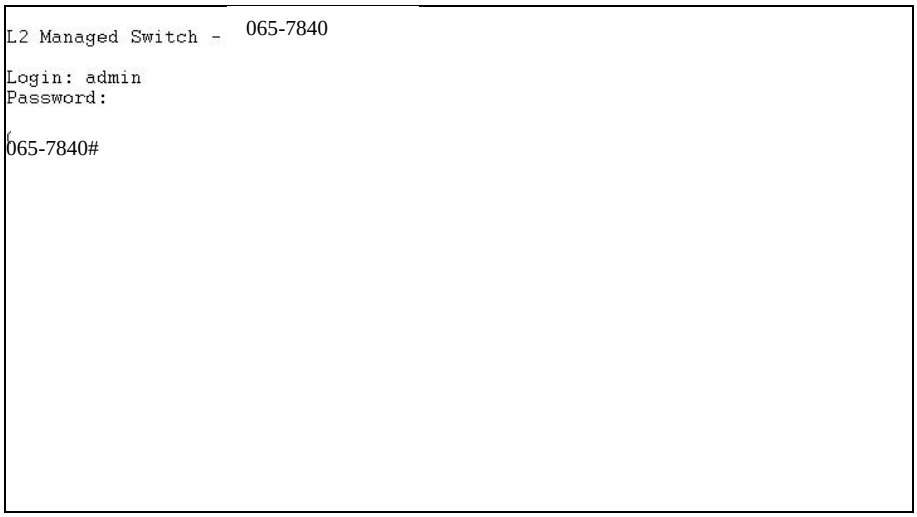


Fig. 2-7 the CLI Login Screen

2-1-3-2. Configuring the Management Agent of the 065-7840 Managed Switch through the Ethernet Port

There are three ways to configure and monitor the switch through the switch's Ethernet port: the CLI, a Web browser, and an SNMP manager. The user interface for the last one is NMS dependent and is not covered here. The first two types of management interface are discussed in this manual.

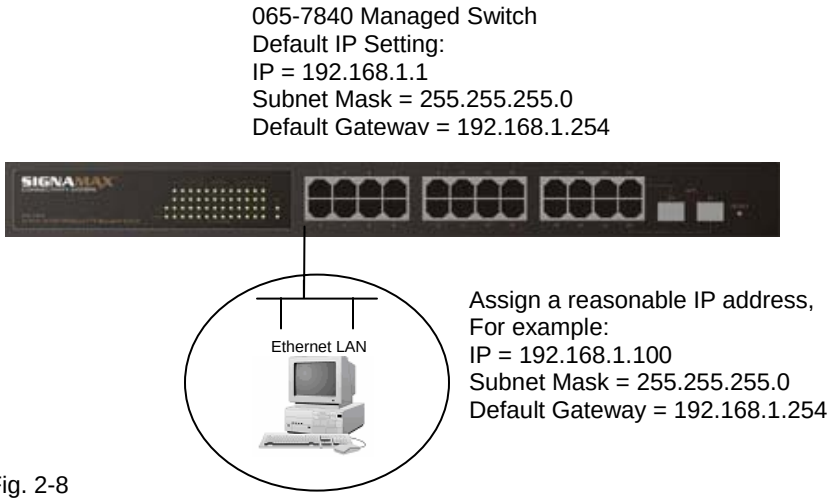


Fig. 2-8

• Managing the 065-7840 Managed Switch through the Ethernet port

Before you communicate with the switch, you have to finish the reconfiguration of the IP address, or you must know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured switch and a PC via a qualified UTP Cat. 5 or better cable with an RJ-45 connector.

   Note: If the PC directly connects to the switch, you have to setup the same subnet mask for both of them. But the subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-8 about the switch's default IP address information.

2. Run the CLI or web browser and follow the menu. Please refer to Chapter 3 and Chapter 4.

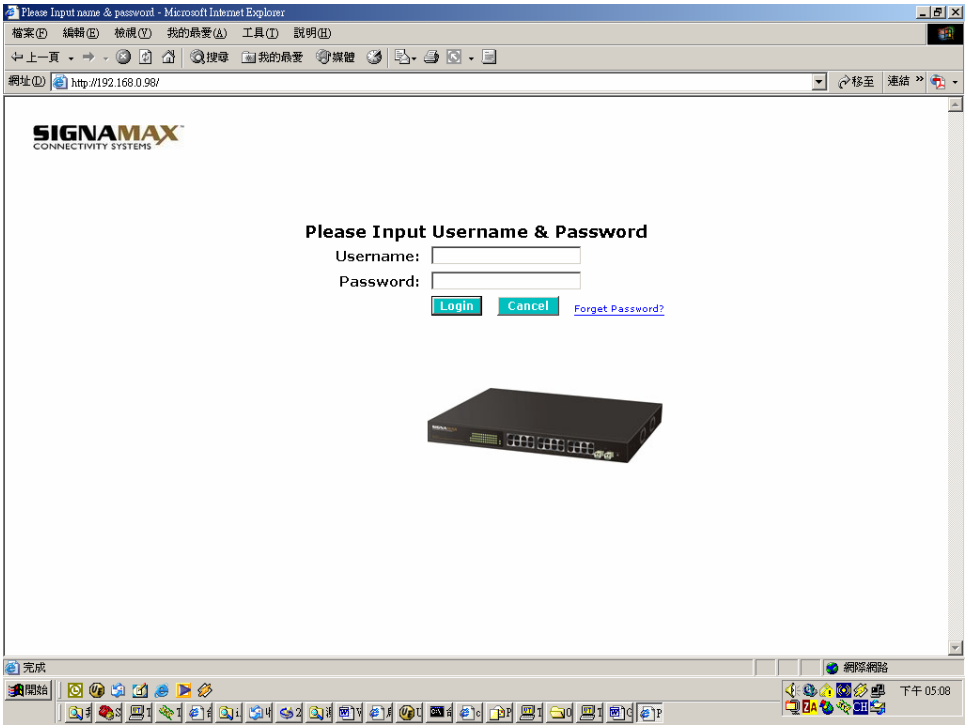


Fig. 2-9 Login Screen for the Web-Based GUI

2-1-4. IP Address Assignment

For the IP address configuration, there are three parameters that need to be established. They are the IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks is shown in the Fig. 2-10. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bit address schema. Each IP address is comprised of two parts: the network identifier (address) and the host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of the host refers to. The host identifier must be unique in the same LAN. The version of the IP address used by the 065-7840 switch is version 4, known as IPv4.

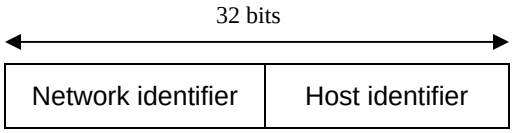
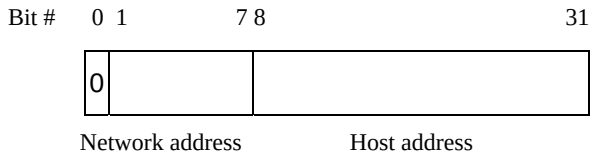


Fig. 2-10 IP address structure

Classful addressing divides the IP address into three classes, class A, class B and class C. The rest of the IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

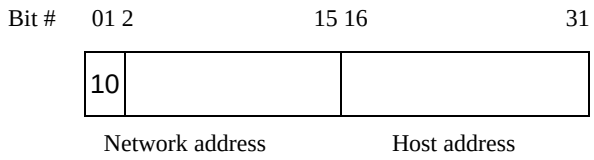
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks that can be defined, because the address 0.0.0.0 is reserved for the default route and 127.0.0.0/8 is reserved for the loopback function.



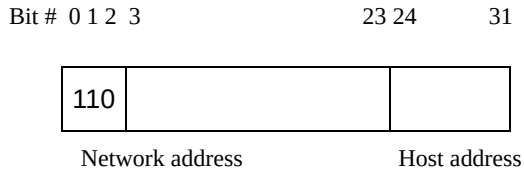
Class B:

IP addresses range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed by a 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined, with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP addresses range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed by an 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with the first 4 MSB (Most significant bits) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with the first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

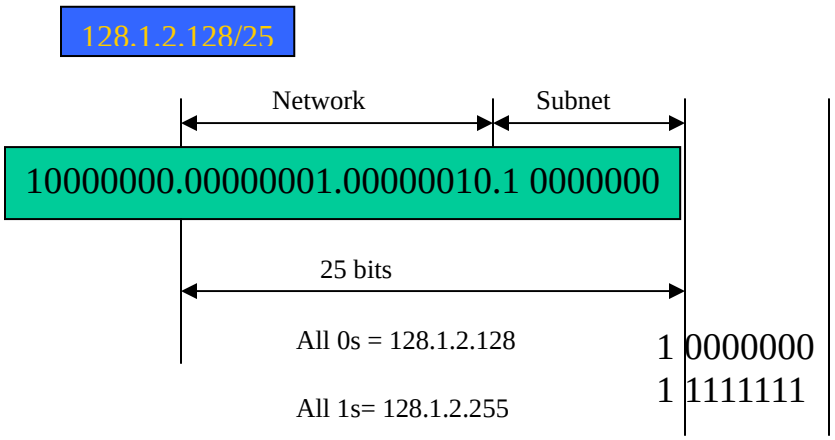
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

The Subnet mask is the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address on a bitwise basis. It is designed to utilize IP addresses more efficiently and provide an easier to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes contain all 1's. This means more than 60 thousand nodes in a flat IP address can reside on the same network. It's too large to manage practically. Now, if we divide it into smaller networks by extending the network prefix from 16 bits to, say, 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP addresses are available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's, plus the host number. For example, for an IP address of 128.1.2.128, what will the IP addresses reserved look like? All 0's mean the network itself, and all 1's mean IP broadcast.



In this diagram, you can see the subnet mask that is 25 bits long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1's in that subnet mask. Using this knowledge, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-4

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class of C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may look like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent subdivided networks in an enterprise network, a partition to the network must be performed. In this case, a subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For a routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as the default router. Basically, it is a routing policy.

In order to assign an IP address to the switch, you have to check what the IP address of the network will be that is connected with the switch. Use the same network address and append your host address to it.

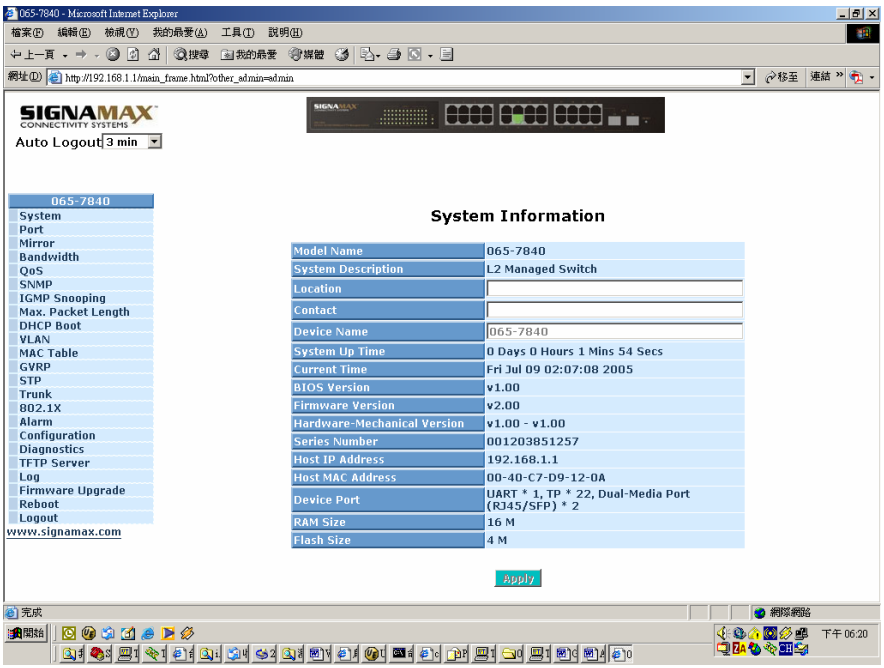


Fig. 2-11

First, the IP Address: as shown in the Fig. 2-11, enter “192.168.1.1”, for instance. For sure, an IP address such as 192.168.1.x ***must*** be set on your PC to be able to communicate with the switch.

Second, the Subnet Mask: as shown in the Fig. 2-11, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

DNS:

The Domain Name Server translates a human readable machine name to an IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, a user generally uses the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

2-2. Typical Applications

The 065-7840 Managed Switch implements 24 Gigabit Ethernet TP ports with auto MDIX and two slots for the removable modules supporting a variety of fiber connection types, including LC and BiDi-LC SFP modules. For more details on the specifications of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central Site/Remote site application, as used in a carrier or an ISP (See Fig. 2-12)
- Peer-to-peer application, as used in two remote offices (See Fig. 2-13)
- Office network (See Fig. 2-14)

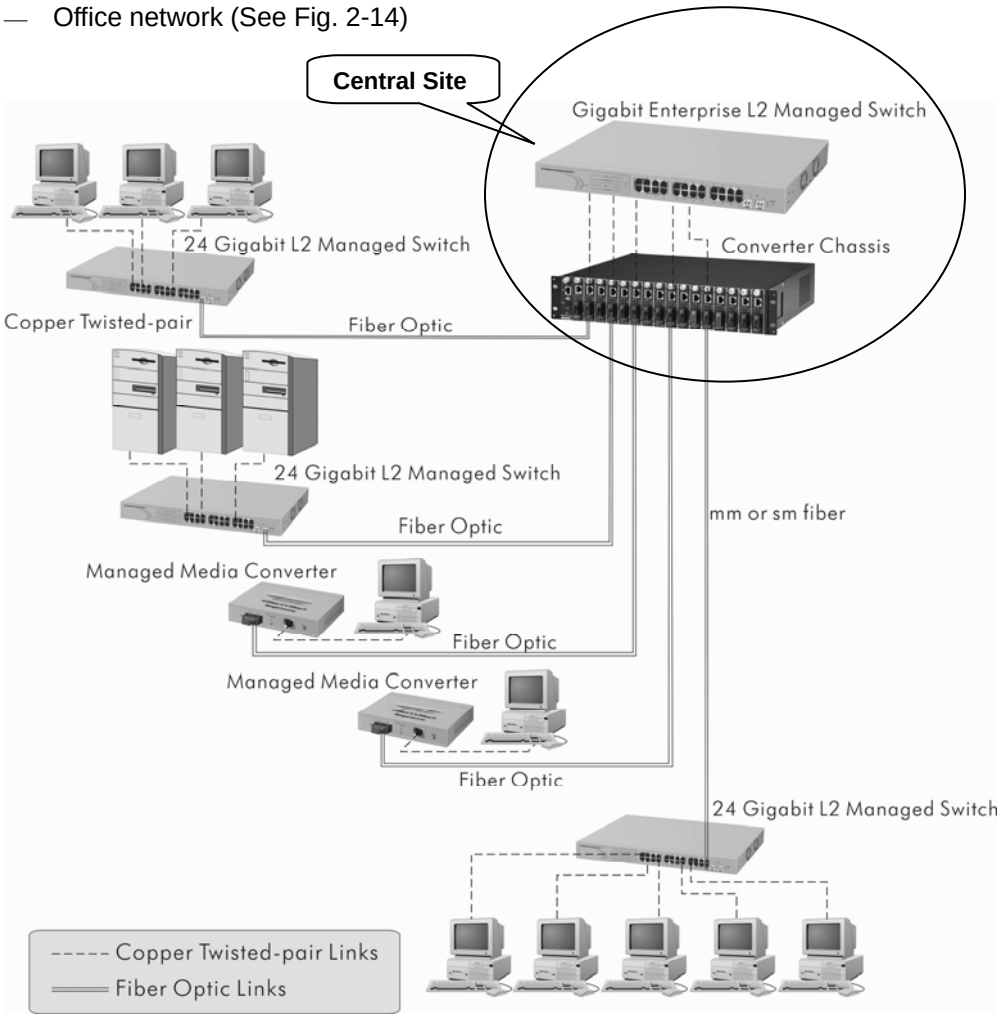


Fig. 2-12 Network Connection between Remote Site and Central Site

Fig. 2-12 is a system-wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

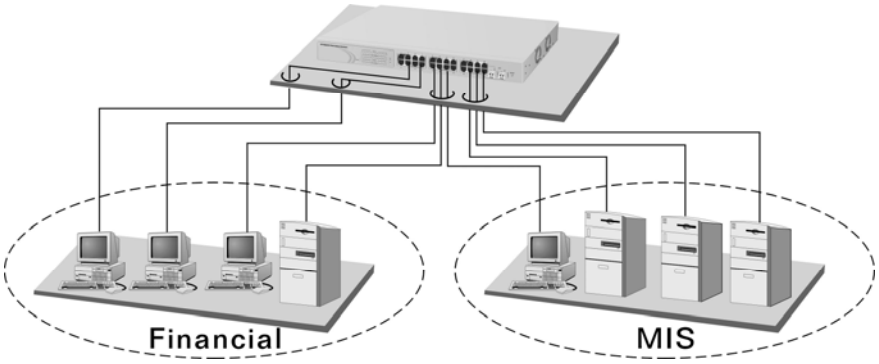


Fig. 2-13 Peer-to-peer Network Connection

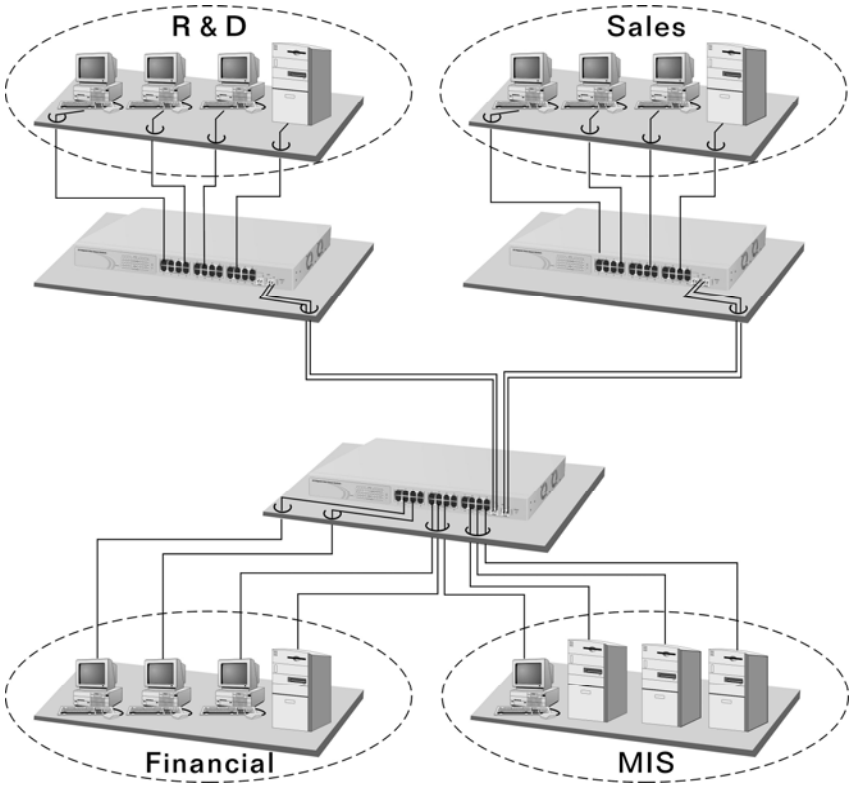


Fig. 2-14 Office Network Connection

3. Operation of Web-based Management

This chapter instructs you how to configure and manage the 065-7840 managed switch through the web user interface it supports, in order to access and manage the 22-Port 10/100/1000 Mbps TP ports and the 2 Gigabit TP/SFP Fiber ports in the switch. With this facility, you can easily access and monitor through any one port of the switch all the statuses of the switch, including MIB statuses, each port's activity, Spanning Tree status, port aggregation status, multicast traffic, VLAN and priority status, and even illegal access records and so on.

The default values of the Signamax 065-7840 managed switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

Table 3-1

After the managed switch has been configured in the CLI via the switch's serial interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Fig.3-1) and ask you to input your username and password in order to login and access authentication. The default username and password are both "admin". For the first use, please enter the default username and password, and then click the **<Login>** button. The login process now is completed.

In this login menu, you have to input the complete username and password respectively; the switch will not give you a shortcut to the username automatically. This looks inconvenient, but it is safer.

The switch supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logs in first to configure the system. The rest of users, even with an administrator's identity, can only monitor the system. Those who have no administrator's identity can only monitor the system at any time. There are a maximum of only three users able to log in to the switch simultaneously.

To optimize the display, Signamax recommends that you use Microsoft IE and have the 1024x768 resolution set for your monitor.

The following pages describe the entire function tree using the web-based user interface. We will navigate through it in this chapter.

Fig. 3-1

3-1. Web Management Home Overview

After you login, the switch shows you the system information as shown in Fig. 3-2. This page is the default and tells you the basic information of the system, including “Model Name”, “System Description”, “Location”, “Contact”, “Device Name”, “System Up Time”, “Current Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Series Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size” and “Flash Size”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful if there is a malfunction.

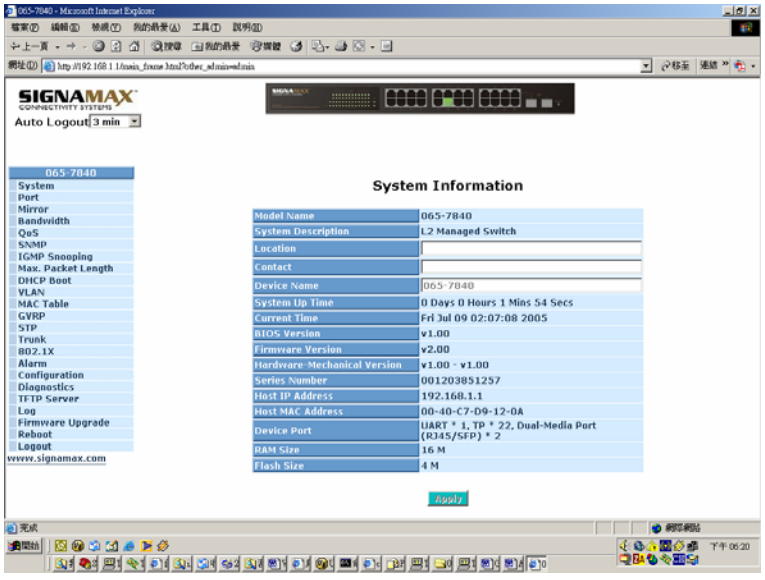


Fig. 3-2

- **Page Layout Information**

— On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; the ports which are not linked will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of the module depends on the one you inserted. The same link indications apply. If disconnected, the port will show as dark; if linked, the port will show as green.

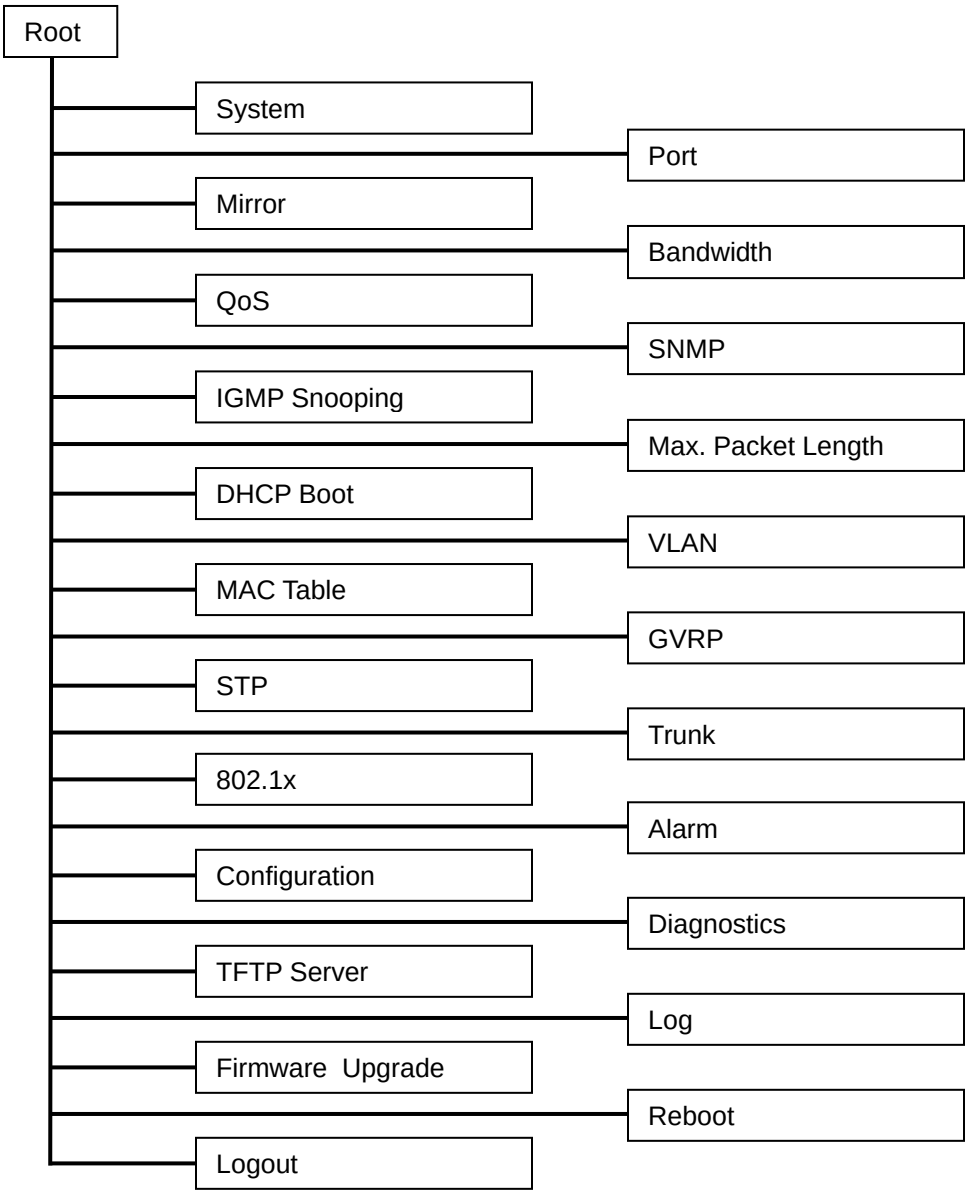
In this device, there are mouse-click functions on the panel provided for the information relating to the ports. These are very convenient functions for browsing the information of a single port. When clicking the port on the front panel, an information window for the port will pop up. (See Fig. 3-3)

Fig. 3-3 Port status information

In Fig. 3-3, it shows the basic information of the selected port. With this, you'll see the information about port status, traffic status and bandwidth rating for egress and ingress respectively.

— On the left top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal users as you are leaving. If you do not choose any selection in the Auto Logout list, it means you've turned on the Auto Logout function, and the system will be logged out automatically if no action is seen on the device after 3 minutes. If OFF is chosen, the screen will remain as it is. Default is ON.

— On the left side, the main menu tree for the web interface is listed on the page. They are hierarchical menus. Open the function folder, and a sub-menu will be shown. The functions of each folder are described in their corresponding sections, respectively. The function is performed when mouse-clicked. The following list is the full function tree for the web-based user interface:


Root
System
Port
Mirror
Bandwidth
QoS
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1x
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout

3-1-1. System Information

Function name:

System Information

Function description:

Show the basic system information.

Parameter description:

Model name:

The model name of this device.

System description:

As it is, this tells what this device is. Here, it is “L2 Managed Switch”.

Location:

The place where this switch is located. User-defined.

Contact:

For easily management and maintenance of this device, you may write down the name and phone number of the contact person who will help you. You can configure this parameter through the device’s user interface or SNMP.

Device name:

The name of the switch. User-defined. Default is 065-7840.

System up time:

The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

Current time:

Show the system time of the switch. Its format: day of week, month, day, hours: minutes: seconds, year. For instance, Wed, Apr. 23, 12:10:10, 2004.

BIOS version:

The version of the BIOS in this switch.

Firmware version:

The firmware version in this switch.

Hardware-Mechanical version:

The Hardware version and Mechanical version of the switch. The figure before the hyphen is the version of the electronic hardware; the one after the hyphen is the mechanical version.

Series number:

The serial number is assigned by the manufacturer.

Host IP address:

The IP address of the switch.

Host MAC address:

It is the Ethernet MAC address of the management agent in this switch.

Device Port:

Show all types and numbers of the port in the switch.

RAM size:

The size of the DRAM in this switch.

Flash size:

The size of the flash memory in this switch.

3-1-2. IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, the network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via a DHCP server. When the IP address is changed, you must reboot the switch to have the setting take effect and use the new IP address to browse for web management and CLI management.

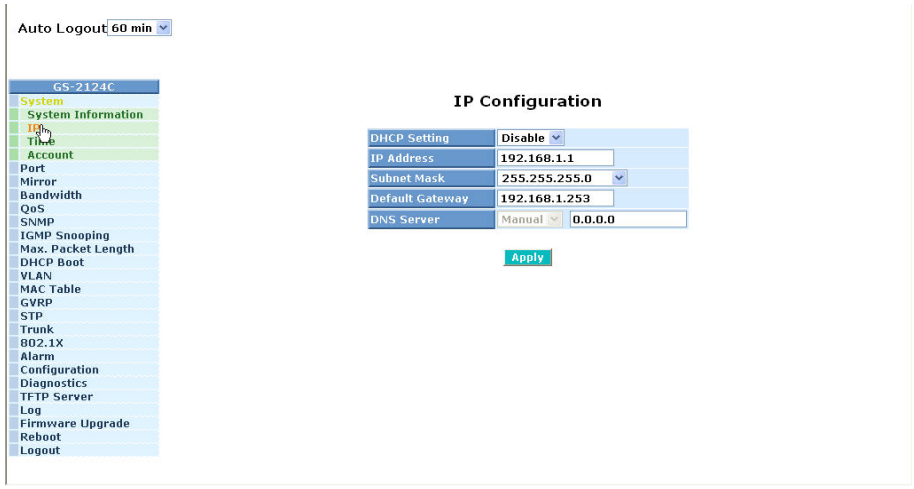


Fig. 3-4 IP Address Configuration

Function name:

IP Configuration

Function description:

Set IP address, subnet mask, default gateway and DNS for the switch.

Parameter description:

DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn the function ON or OFF.

The switch supports a DHCP client used to get an IP address automatically if you set this function to “Enable”. When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show that the IP address is under request until the DHCP server is up. Before getting an IP address from a DHCP server, the device will not continue booting procedures. If this field is set to “Disable”, you’ll have to input the IP address manually. For more details about IP addresses and DHCP, please see Section 2-1-4, “IP Address Assignment”, in this manual.

Default: Disable

IP address:

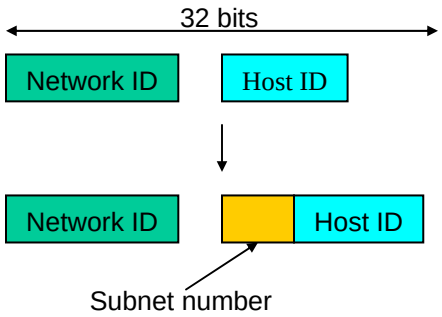
Users can configure the IP settings and fill in new values if users set the DHCP function to “Disable”. Then, click the **<Apply>** button to update.

When DHCP is disabled, the Default IP Address is: 192.168.1.1

If DHCP is enabled, this field is filled by the DHCP server and will not allow the user to manually set it.

Subnet mask:

Subnet mask is made for the purpose of getting more network addresses, because any IP device in a network must own its IP address, composed of a Network address and a Host address, otherwise it can’t communicate with other devices. Unfortunately, the network classes A, B, and C are all too large to fit for almost all networks; hence, a subnet mask is introduced to solve this problem. A Subnet mask uses some bits from the host address and makes an IP address look like a Network address, Subnet mask number and host address. This is shown in the following figure. This reduces the total number of IP addresses a network able to support, by the amount of the 2nd power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resident in the same network to which it is attached.

For more information, please also see Section 2-1-4, “IP Address Assignment”, in this manual.

Default: 255.255.255.0

Default gateway:

Sets an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with an undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS:

A DNS, or Domain Name Server, is used to provide the translation between IP addresses and name addresses.

The switch supports DNS client functions to re-route the mnemonic name address to the DNS server to get its associated IP address for accessing the Internet. The user can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by the DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default value is no assignment of the DNS address.

Default: 0.0.0.0

3-1-3. Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple; just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. The version of NTP, an internet draft standard formalized in RFC 1305, that has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resident in the Internet and a user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Function name:

Time

Function description:

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving time for a different area’s time adjustment.

Parameter description:

Current Time:

Show the current time of the system.

Manual:

This is the function that adjusts the time manually. By filling valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and pressing the **<Apply>** button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. If you input the wrong figure and press the **<Apply>** button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1
Hour = 0, Minute = 0, Second = 0

NTP:

NTP is Network Time Protocol and is used to sync the network time based upon Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify a user-defined NTP server as well as a Time Zone, the switch will sync the time shortly after pressing the **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user processing.

Time Zone is an offset time from GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and the updated NTP time to determine the local time, otherwise you will not able to get the correct time. The switch supports configurable time zones from –12 to +13 1 hour steps.

Default Time zone: + 8 Hrs.

Daylight Saving:

Daylight savings time is adopted in some countries. If set, it will adjust the time lag or advance in units of hours, according to the starting date and the ending date. For example, if you set the daylight saving to be 1 hour, when the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means the switch need not adjust the current time, which is equivalent to inactive daylight saving. You do not have to set the starting/ending date, as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Daylight Saving Start:

This is used to set when to start performing the daylight saving time adjustment.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Daylight Saving End:

This is used to set when to stop performing the daylight saving time adjustment.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

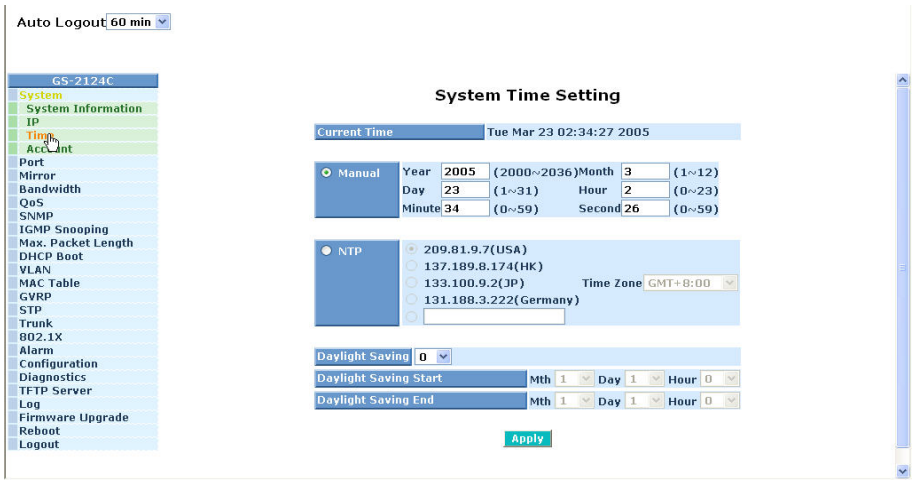


Fig. 3-5

3-1-4. Account Configuration

Using this function, only the administrator can create, modify or delete the username and password. The administrator can modify other guest identities' password without confirming the password, but it is necessary to modify the administrator-equivalent identity. A guest-equivalent identity can modify that password only. Please note that you must confirm administrator/guest identity in the Authorization field in advance before configuring the username and password. Only one administrator is allowed to exist and is unable to be deleted. In addition, up to 5 guest accounts can be created.

The default setting for user account is:

Username: admin
Password: admin

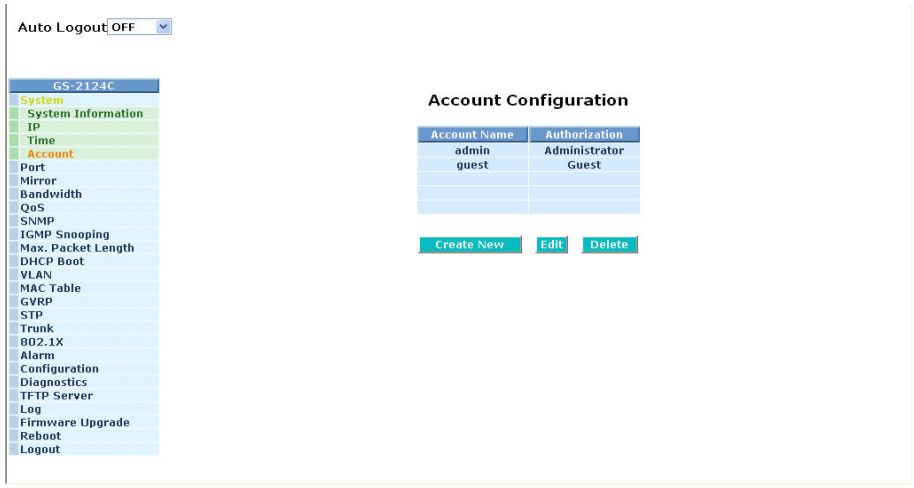
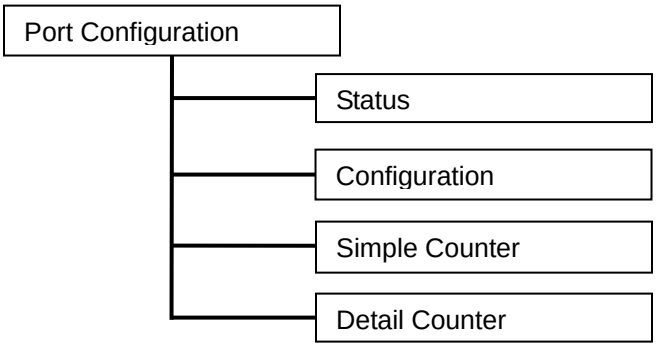


Fig. 3-6

3-2. Port Configuration

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in this function folder for port monitoring and management. Each of them will be described in detail in the following sections.



3-2-1.Port Status

The Port Status function gathers the information of all ports' current status and reports it by the order of port number, link status, port state, Auto-Negotiation status, speed/duplex and flow control. Extra media-specific information for the SFP module ports 23 and 24 is also offered (See Fig. 3-8).

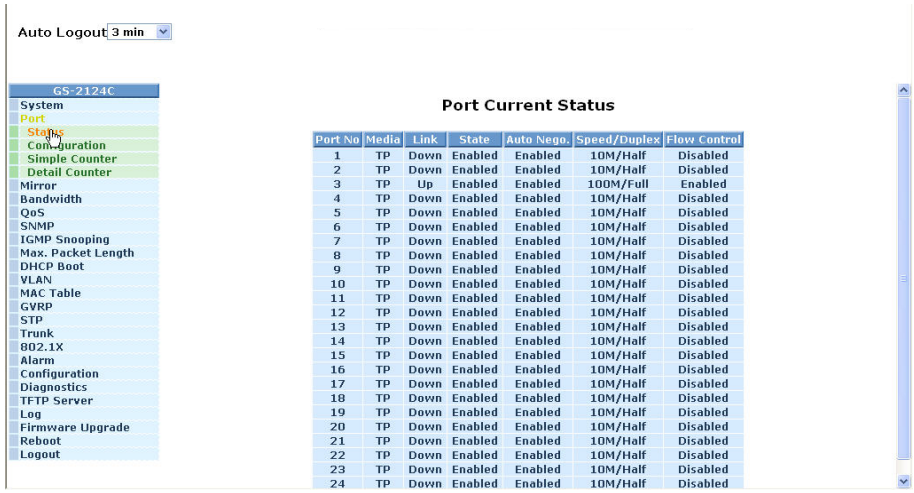

Auto Logout 3 min
GS-2124C
System
Port
Status
Configuration
Simple Counter
Detail Counter
Mirror
Bandwidth
QoS
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Port Current Status
Port No | Media | Link | State | Auto Nego. | Speed/Duplex | Flow Control
1 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
2 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
3 | TP | Up | Enabled | Enabled | 100M/Full | Enabled
4 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
5 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
6 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
7 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
8 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
9 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
10 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
11 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
12 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
13 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
14 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
15 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
16 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
17 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
18 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
19 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
20 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
21 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
22 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
23 | TP | Down | Enabled | Enabled | 10M/Half | Disabled
24 | TP | Down | Enabled | Enabled | 10M/Half | Disabled

Fig. 3-7

Function name:

Port Status

Function Description:

Reports the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter as displayed in the page, the port current status will be automatically refreshed about every 5 seconds.

Parameter Description:

Port No:

Displays the port number. The number is 1 – 24. Both port 23 and 24 can be equipped with optional SFP modules.

Media:

Shows the media type used in all ports. Port 23 and Port 24 are equipped to utilize optional SFP modules, allowing these two ports to support either fiber or UTP media with either Gigabit Ethernet (1000 Mbps) or 10/100Mbps Fast Ethernet port. These two ports may have different media types and speeds. The fiber port supports different types of connectors, distances, fiber modes, etc. The switch describes the module ports, as shown on the following pages.

Link:

Indicates if the link on the port is active or not. If the link is connected to a properly-working device, the Link status will show the link “Up”; otherwise, it will show “Down”. This is determined by the hardware devices on both ends of the connection.

No default value.

State:

Shows that the communication function of the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. The Port State is configured by the user.

Default: Enabled.

Auto Negotiation:

Shows the exchange mode of an Ethernet MAC-addressed device. There are two modes supported in the switch. They are auto-negotiation mode “Enabled” and forced mode “Disabled”. When in “Enabled” mode, this function will automatically negotiate by the hardware of the connected devices themselves, and exchange with each other the capability of speed and duplex mode with the other device which is linked, determining the best communication speed and duplex mode. When in “Disabled” mode, both device must have the same setting of speed and duplex mode; otherwise, they will not be linked. In this case, the link result is “Down”.

Default: Enabled

Speed / Duplex Mode:

Displays the speed and duplex mode of all ports. There are three speeds (10 Mbps, 100 Mbps and 1000 Mbps) supported for TP media, and the duplex modes supported are half duplex and full duplex. If the media is 1 Gbps fiber, the 1000 Mbps speed is the only one supported. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in “Auto Speed” mode or 2) user setting in “Force” mode. The local port has to have its capability preset.

Default: None, depends on the result of the negotiation.

Flow Control:

Shows each port’s flow control status.

There are two types of flow control in Ethernet: Backpressure for half-duplex operation, and Pause flow control (IEEE802.3x) for full-duplex operation. The switch supports both of these types of flow control.

Default: Disabled

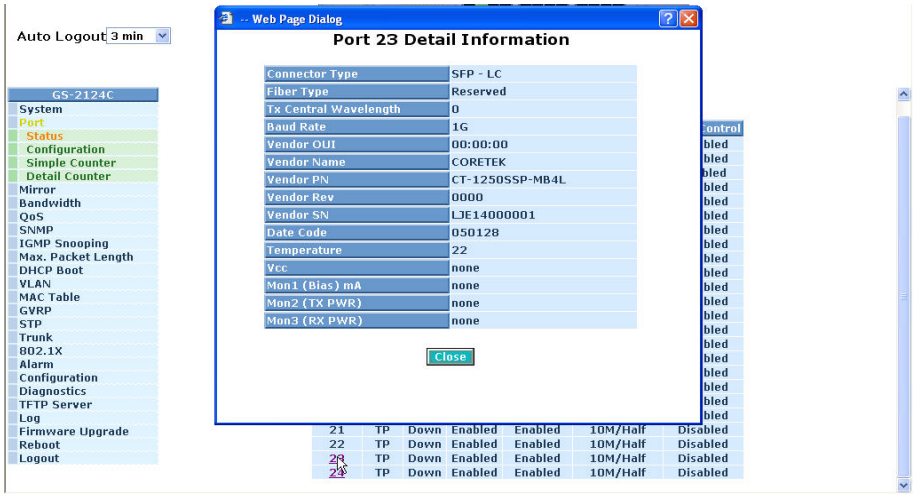


Fig. 3-8

Parameter description of Port 23 and Port24:

Connector Type:

Displays the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type:

Displays the fiber mode, for instance, Multimode, Singlemode.

Tx Central Wavelength:

Displays the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:

Displays the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G, 10G and so on.

Vendor OUI:

Displays the Manufacturer's OUI code which is assigned by IEEE.

Vendor Name:

Displays the company name of the module manufacturer.

Vendor P/N:

Displays the product name provided by the module manufacturer.

Vendor Rev (Revision):

Displays the module revision.

Vendor SN (Serial Number):

Shows the serial number assigned by the manufacturer.

Date Code:

Shows the date this SFP module was made.

Temperature:

Shows the current temperature of the SFP module.

Vcc:

Shows the working DC voltage of the SFP module.

Mon1 (Bias) mA:

Shows the Bias current of the SFP module.

Mon2 (TX PWR):

Shows the transmit power of the SFP module.

Mon3 (RX PWR):

Shows the received power of the SFP module.

3-2-2. Port Configuration

Port Configuration is applied to change the setting of each port. By using this configuration capability, you can set/reset the following functions. All of them are described in detail below.

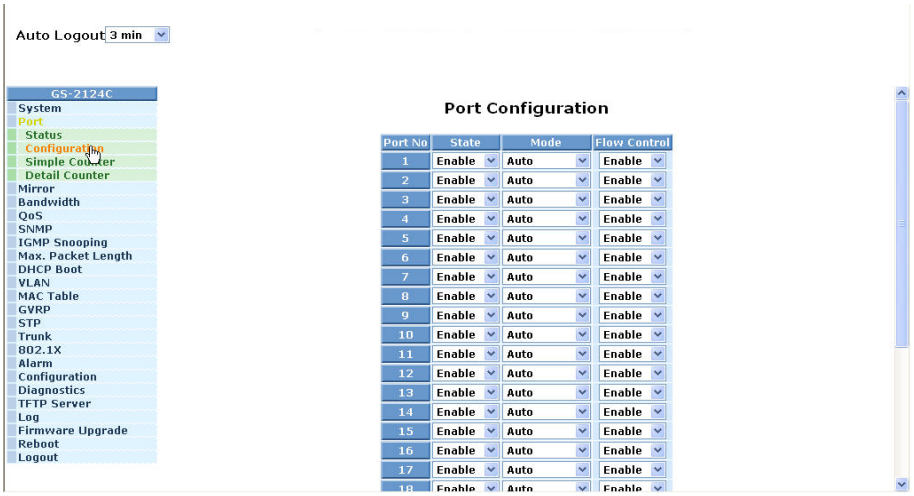


Fig. 3-9

Function name:

Port Configuration

Function description:

Used to set each port's operation mode. The switch supports 3 parameters for each port. They are state, mode and flow control.

Parameter description:

State:

Sets the communication capability of the port to Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states "Enable" and "Disable" able to be chosen. If you set a port's state to "Disable", then that port is prohibited to pass any traffic, even if its Link is up.

Default: Enable.

Mode:

Set the speed and duplex of the port. In speed, if the media is 1 Gbps fiber, it is always 1000 Mbps and the only duplex mode permitted is full. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000 Mbps, and duplex mode, either full duplex or half duplex. The following table summarizes the functions the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto-negotiation mode, there is no default value. In Forced mode, default value depends on your settings.

Flow Control:

There are two modes to choose from in flow control, either Enable or Disable. If flow control is set to Enable, both parties can send a PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if the traffic is too much to handle.

Default: Enable.

3-2-3. Simple Counter

The function of Simple Counter is to collect any information and provide the traffic counts of the port, no matter whether the packet is good or bad.

In the Fig. 3-10, the window can show all ports' counter information at the same time. Each data field is 12 digits long. If the counters overflow, the counter will be reset and will restart counting. The data is updated every time interval as defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

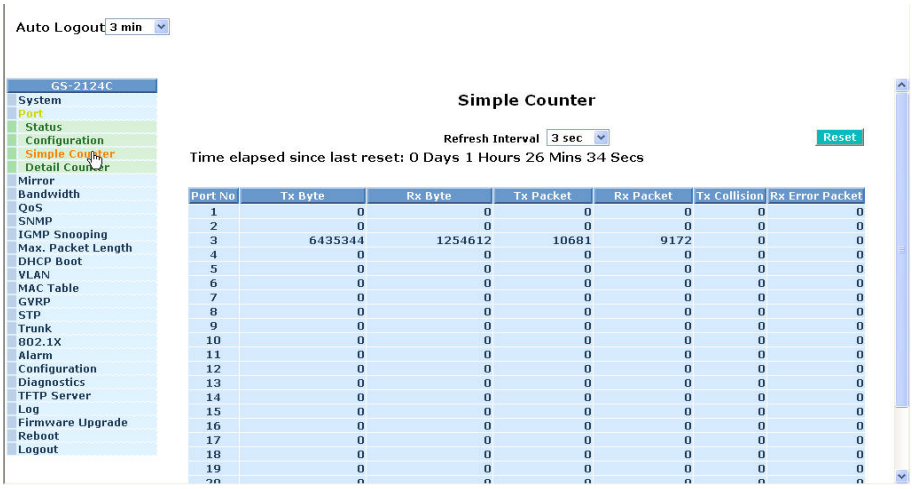

Auto Logout 3 min
GS-2124C
System
Port
Status
Configuration
Simple Counter
Detail Counter
Mirror
Bandwidth
QoS
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Simple Counter
Refresh Interval 3 sec
Reset
Time elapsed since last reset: 0 Days 1 Hours 26 Mins 34 Secs
Port No | Tx Byte | Rx Byte | Tx Packet | Rx Packet | Tx Collision | Rx Error Packet
1 0 0 0 0 0 0
2 0 0 0 0 0 0
3 6435344 1254612 10681 9172 0 0
4 0 0 0 0 0 0
5 0 0 0 0 0 0
6 0 0 0 0 0 0
7 0 0 0 0 0 0
8 0 0 0 0 0 0
9 0 0 0 0 0 0
10 0 0 0 0 0 0
11 0 0 0 0 0 0
12 0 0 0 0 0 0
13 0 0 0 0 0 0
14 0 0 0 0 0 0
15 0 0 0 0 0 0
16 0 0 0 0 0 0
17 0 0 0 0 0 0
18 0 0 0 0 0 0
19 0 0 0 0 0 0

Fig. 3-10

Function name:

Simple Counter

Function description:

Displays the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

Parameters description:

Tx Byte:

Total transmitted bytes.

Rx Byte:

Total received bytes.

Tx Packet:

The counted number of packets transmitted.

Rx Packet:

The counted number of packets received.

Tx Collision:

Number of collisions transmitting frames experienced.

Rx Error Packet:

Number of bad packets received.

3-2-4. Detail Counter

The function of Detail Counter collects any information and provides the counts concerning the traffic of the port, no matter if the packets are good or bad.

As shown in Fig. 3-11, the window can show only one port counter information at the same time. To see another port's counter, pull down the Select list, and then the figures displayed relate to the port chosen.

Each data field is 12 digits long. If the counter overflows, the counter will be reset and will restart counting. The data is updated every time interval as defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

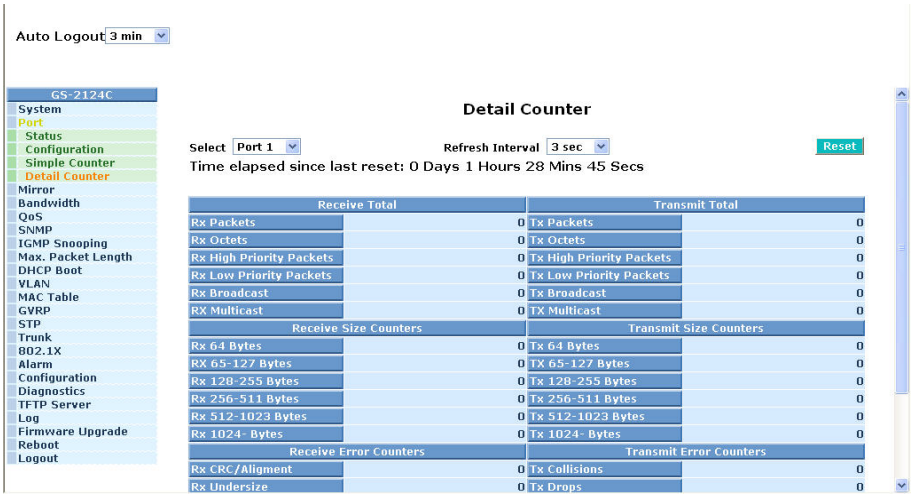


Fig. 3-11

Function name:

Detail Counter

Function description:

Displays the detailed count number of each port's traffic. As shown in Fig. 3-11, the window can show all counter information of each port at one time.

Parameter description:

Rx Packets:

The counted number of packets received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

The counted number of broadcast packets received.

Rx Multicast:

The counted number of multicast packets received.

Tx Packets:

The counted number of packets transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

The counted number of broadcast packets transmitted.

Tx Multicast:

The counted number of multicast packets transmitted.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames (according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames (according to max_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receive buffer space.

Rx Errors:

Number of errored packets received.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops:

Number of frames dropped due to the lack of transmit buffer space.

3-3. Mirror

Function name:

Mirror Configuration

Function description:

Mirror Configuration is used to monitor the traffic of the network. For example, we assume that Port A and Port B are the Monitoring Port and Monitored Port respectively; thus, the traffic received by Port B will be copied to Port A for monitoring.

Parameter description:

Mode:

Used for the activation or deactivation of the Port Mirror function. Default is "disable".

Monitoring Port:

Set up the port for monitoring. Valid port is Port 1~24 and default is Port 1.

Monitored Port:

Set up the port for being monitored. Just tick the check box (☑) beside the port x and valid port is Port 1~24.

Fig. 3-12

3-4. Bandwidth Management

Function name:

Bandwidth Management

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

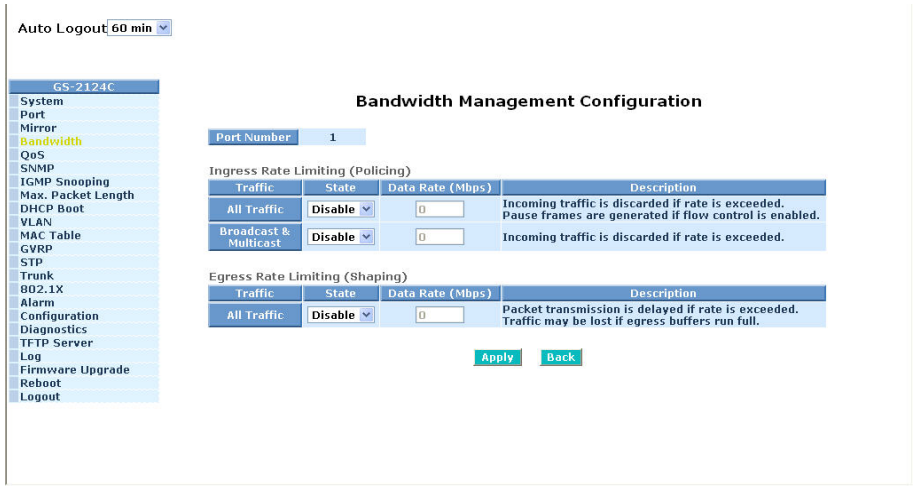


Fig. 3-13

Parameter description:

Port Number:

Choose the port on which you would like this function to operate. Valid range of the port is 1~24.

All Traffic for Ingress Rate Limiting (Policing):

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

Broadcast & Multicast for Ingress Rate Limiting (Policing):

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. The format of the packet limits to broadcast and multicast. Valid range is 0~1000.

All Traffic for Egress Rate Limiting (Shaping):

Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

3-5. QoS (Quality of Service) Configuration

The switch offers 5 powerful kinds of QoS functions. There are Per Port Priority so that you can assign each port to a different precedence; VLAN Tag priority, so that you can assign precedence of up to 8 priorities; IP TOS Classification; IP TCP/UDP Port Classification; and IP DiffServ Classification.

In Quality of Service (QoS) Configuration, there is one option named ”Default Class”. As you had selected one of the five QoS functions, then some packets that did not belong to this QoS setting would be viewed as Default Class. For instance, if you set the QoS function as VLAN Tag Priority mode, and then choose Default Class as High, then the priority of the packets with no tag will be considered as High priority precedence. The initial value of the Default Class is High.

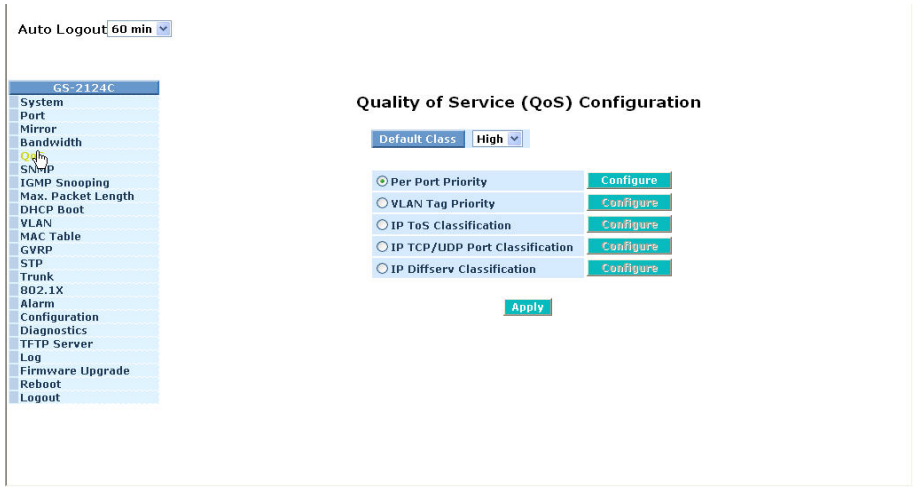


Fig. 3-14

Function name:

Per Port Priority

Function description:

Allows assignment of QoS Priority High and Low for each port. For example, if IP packets are transmitted from Port 2 and Port 3 at the speed of 1 Gbps to Port 1, and the Class of Port 2 is set as High and Port 3 is set as Low, then the packets of Port 3 will be dropped if congestion occurs because Port 2 has a higher precedence of transmitting packets.

Parameter description:

Port No:

User can choose the port (1~24) respectively with Priority Class on Per Port Priority function.

Class:

User can set up High Priority or Low Priority for each port respectively.

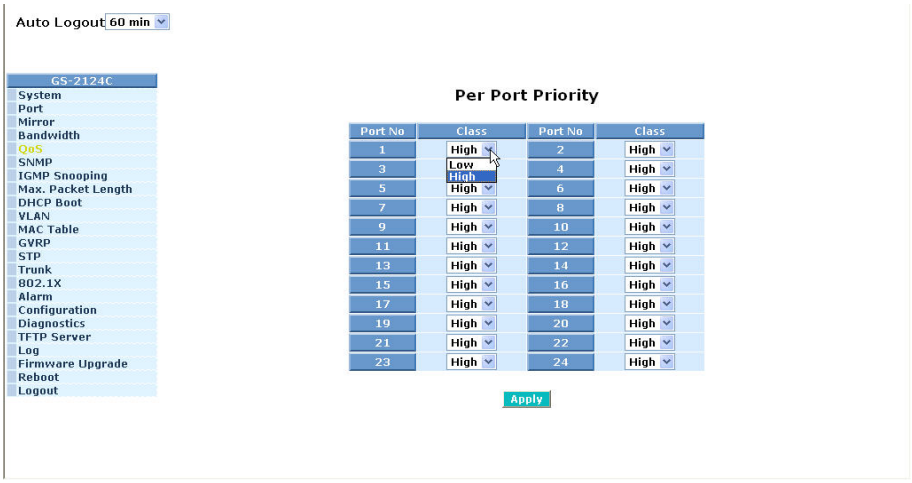


Fig. 3-15

Function name:

VLAN Tag Priority

Function description:

In VLAN tagging, there are 3 bits belonging to priority. According to these 3 bits, we could arrange 8 traffic classes –0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0, 1 1 1. We can set High priority or Low priority for each traffic class. For instance, let us let VLAN-tagged priority 0 0 0 be high priority and VLAN-tagged priority 0 0 1 be Low Priority, and then assign ports 1, 2, 3 to reside in VLAN 2. Packets are sent to ports 2 and 3 that have VLAN-tagged Field assigned as 0 0 0 and VID equals 2 from the port 2 and the packets that have VLAN-tagged Field appears 0 0 1 and VID equals 2 from the port 3. We let the two kinds of packets be transmitted to port 1 until the port results in congestion. The result is that the packets will be dropped partially from port 3, because the packets that emanate from there are assigned Low Priority. To use the VLAN Tag Priority function, please press the **<Configure>** button at the right section

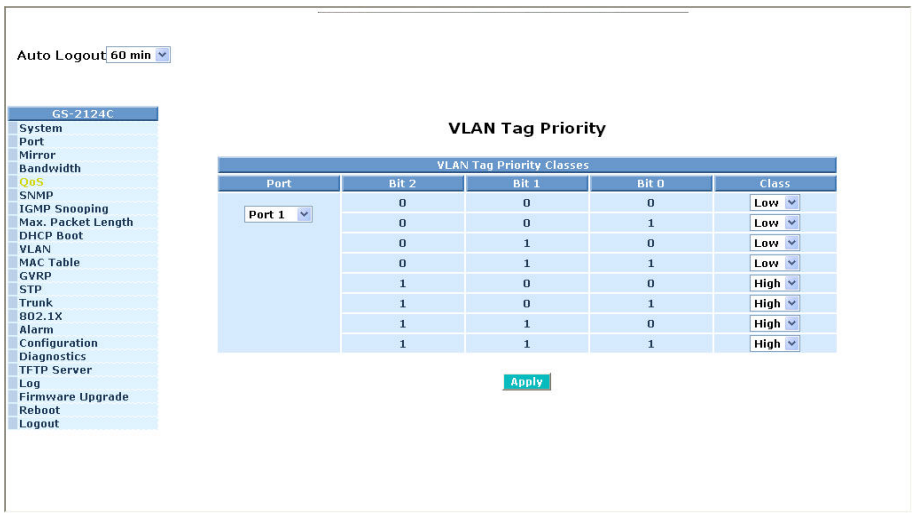


Fig. 3-16

Parameter description:

Quality of Service (QoS) VLAN Tag Configuration:

Used for setting up the QoS belonging to VLAN operation.

Port:

User can set up the port (1~24) respectively to let the VLAN Tag QoS function operate on them. If it is desirable to set up all ports at a time, the user is also allowed to choose “All” in the selection list to simplify the configuration procedure.

Bit 0, Bit 1, Bit 2:

According to the arrangement of VLAN-tagged priority, it can form 8 kinds of traffic classes, including 0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0
and 1 1 1.

Class:

8 kinds of traffic as mentioned above; the user can set up High Priority or Low Priority for each port respectively.

Function name:

IP TOS Classification

Function description:

Another QoS function is the application of Layer 3 on the network framework. This focuses on the TOS field of the IP header. There are three bits in the TOS field. Bits 2~4 of the TOS field are used. According to these 3 bits, 8 traffic classes can be arranged –0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0, 1 1 1. As long as bits 5~7 of the TOS field of the IP header are changed, we will create the 8 traffic packets intended. Moreover, High priority or Low priority can be set for each traffic class. For instance, if we let TOS 0 0 0 be high priority and TOS 0 0 1 be Low Priority, we sent in the packets that have bit 5~7 of TOS Field appear as 0 0 0 from port 2 and the packets that have bit 5~7 of TOS Field appear as 0 0 1 from port 3. We let the two kinds of packets be transmitted to port 1 until the port results in congestion. The result is that the packets will be dropped partially from port 3, because those packets are assigned Low Priority. To use the TOS Priority function, please press the **<Configure>** button at the right section to set it in advance.

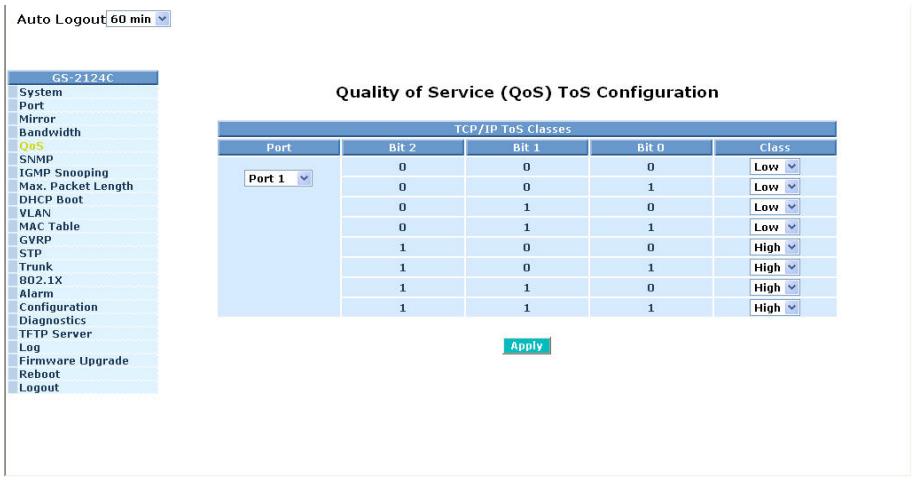


Fig. 3-17

Parameter description:

Quality of Service (QoS) ToS Configuration:

Used for setting up the QoS assignments in Layer 3.

Port:

The user can set up ports (1~24) respectively to let the TOS QoS function operate on them. If it is desirable to set up all ports at a time, the user is also allowed to choose “All” in the selection list to simplify the configuration procedure.

Bit 0, Bit 1, Bit 2:

According to the arrangement of Bit 5 ~ Bit 7 in TOS Field of IP Header, it can form 8 kinds of traffic classes, including 0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

8 kinds of traffic as mentioned above; the user can set up High Priority or Low Priority for each port respectively.

Function name:

IP TCP/UDP Port Classification

Function description:

In L4 QoS Configuration, you can enter a special network transmission event to prioritize it appropriately; for example we use ”Down prioritize web browsing, e-mail, FTP and news“ in the L4 QoS Configuration and click apply, and then click Custom L4. We can find Special TCP/UDP port 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have already existed and are defined for your use, but it is possible for you to modify this pre-defined TCP/UDP port with other port numbers you prefer. In ”Down prioritize web browsing, e-mail, FTP and news“, L4 QoS Configuration with a default setting, specially defined TCP/UDP port possesses a lower QoS traffic than Default class (all other TCP/UDP ports such as port 81,82,83,84,85,etc.). As an example, when we transmit TCP packets with port number 80 from port 2 and port number 81 from port 3 to port 1 until congestion occurs, the packets from port 3 will be dropped by port 1 because the TCP packets have port number 80 assigned as high priority and will havea higher precedence to be forwarded from port 1.

Parameter description:

Disable IP TCP/UDP Port Classification:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to disable IP TCP/UDP port Classification for QoS.

Down prioritize web browsing, e-mail, FTP and news:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize IP Telephony (VoIP):

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize iSCSI:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize web browsing, e-mail, FTP transfers and news:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize Streaming Audio/Video:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function take effect. Then, enter Custom L4 to set up a Special TCP/UDP port for QoS.

Advanced Mode:

Display the TCP/UDP port number in L4 QoS. In “Disable IP TCP/UDP Port Classification” mode, the user can randomly choose a TCP/UDP port number that L4 QoS will affect. As to other special L4 QoS events, Special TCP/UDP port number will be taking action. The user could also be allowed to add or modify the port number at random. For instance, if we choose “Down prioritize web browsing, e-mail, FTP and news” as the QoS of L4 and enter the “Advanced Mode”, then we can see that some special port number 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have been configured already. The user also has the right to modify these port numbers. The display is shown in Fig 3-18.

Special TCP/UDP class:

There are two modes for selection, including Low and High.

Default class (all other TCP/UDP ports):

There are two modes for selection, including Low and High.

Port:

The user can set up the port (1~24) respectively to let Special TDP/UDP class function operate on them. If it is desirable to set up all ports at a time, the user is also allowed to choose “All” in the selection list to simplify the configuration procedure.

Special UDP/TCP Port Selection:

The following are port numbers defined by six specific networks in L4:

- Down prioritize web browsing, e-mail, FTP and news: port number 80,280,443,25,110,20,21,69,119,2009
- Prioritize IP Telephony (VoIP):1718,1719,1720
- Prioritize iSCSI:3225,3260,3420
- Prioritize web browsing, e-mail, FTP transfers and news: 80,280,443,25,110,20,21,69,119,2009
- Prioritize Streaming Audio/Video: 2979,1755,7070,7071,554,8000
- Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):66,1571,1575,523,118,156,3306,1232,1433,1434

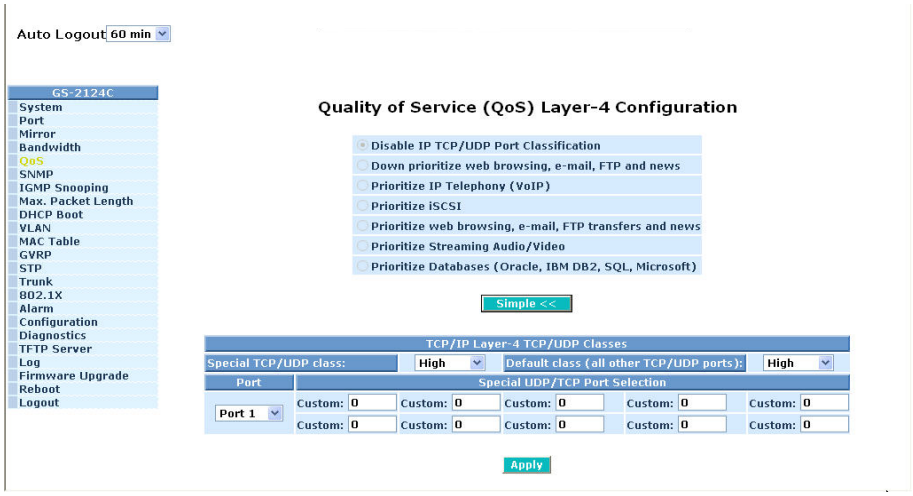


Fig. 3-18 Advanced Mode

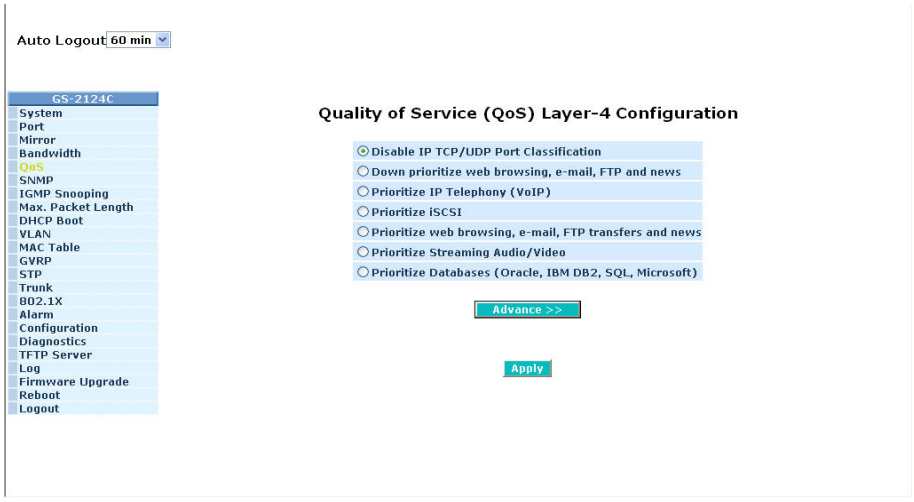


Fig. 3-19 Simple Mode

Simple Mode:

Pressing the **<Simple>** button returns the user to the screen where all L4 port numbers have disappeared (See Fig 3-19).

Function name:

IP DiffServ Classification

Function description:

Using the IP DiffServ Classification function, the switch can form a total of 64 (0~63) kinds of Traffic Class based on the arrangement of the 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to High or Low Priority.

Parameter description:

IP Differentiated Services (DiffServ) Configuration:

Used for setting up the IP Differentiated Services Configuration QoS.

DiffServ:

Display 64 (0~63) DiffServ Priority items.

Class:

64 kinds of traffic as described above; the user can set up High Priority or Low Priority for each port respectively.

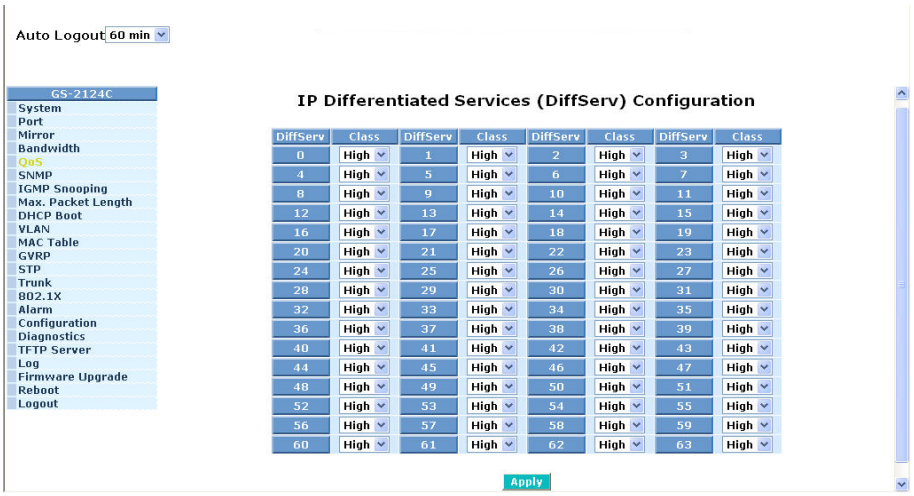

Auto Logout 60 min
GS-2124C
System
Port
Mirror
Bandwidth
QoS
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
IP Differentiated Services (DiffServ) Configuration
DiffServ Class DiffServ Class DiffServ Class DiffServ Class
0 High 1 High 2 High 3 High
4 High 5 High 6 High 7 High
8 High 9 High 10 High 11 High
12 High 13 High 14 High 15 High
16 High 17 High 18 High 19 High
20 High 21 High 22 High 23 High
24 High 25 High 26 High 27 High
28 High 29 High 30 High 31 High
32 High 33 High 34 High 35 High
36 High 37 High 38 High 39 High
40 High 41 High 42 High 43 High
44 High 45 High 46 High 47 High
48 High 49 High 50 High 51 High
52 High 53 High 54 High 55 High
56 High 57 High 58 High 59 High
60 High 61 High 62 High 63 High
Apply

Fig. 3-20

3-6. SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with an SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between the SNMP manager and agent and traverses the Object Identity (OID) of the Management Information Base (MIB), described in the form of SMI syntax. The SNMP agent is running on the switch to respond to the requests issued by the SNMP manager.

Basically, it is passive except when issuing the trap information. The Switch supports an internal switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, the SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via the SNMP manager. If the field SNMP is set as “Disable”, the SNMP agent will be deactivated, and the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. The SNMP manager must pass the authentication by identifying both community names, and then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click the **<Apply>** button, and the setting takes effect.

Parameters description:

SNMP:

The term SNMP here is used for the activation or deactivation of SNMP. Default is "Enable".

Get/Set/Trap Community:

Community name is used as a password for authenticating if the requesting network management unit belongs to the same community group. If they both don’t have the same community name, they don’t belong to the same group. Hence, the requesting network management unit can not access the device with a different community name via SNMP protocol; If they both have the same community name, they can communicate with each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is no blank allowed in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can’t be applied to other function such as SET and Trap.

Default SNMP function: Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function: Enable

Default trap host IP address: 0.0.0.0

Default port number: 162

Trap:

In the switch, there are four trap hosts supported. Each of them has its own community name and IP address, and is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with the SNMP manager receiving the trap message from the managed switch with the switch's SNMP agent issuing the trap message. 6 trap hosts can prevent losing the important trap message from the switch.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap occurs. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap, it is classified as a private trap, which are listed in the Trap Alarm Configuration function folder.

Default for all public traps: Enable.

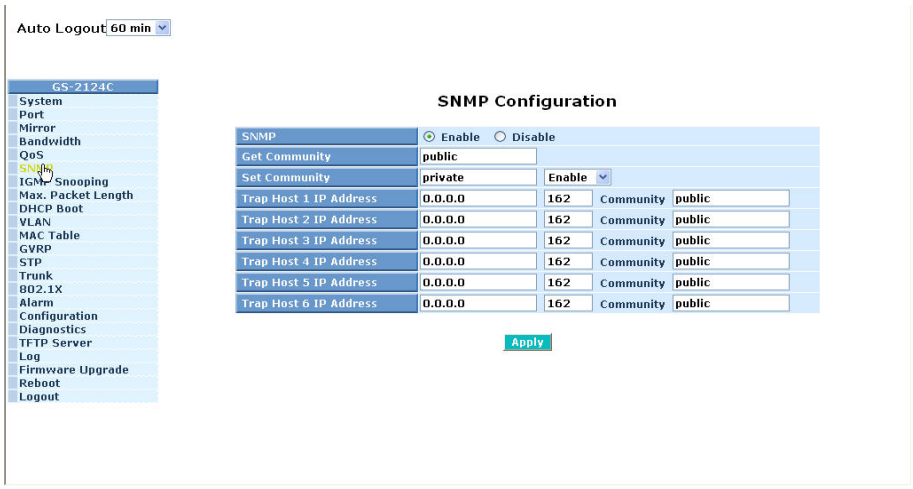


Fig. 3-21 Community and trap host setting

3-7. IGMP Snooping

The IGMP Snooping function is used to establish multicast groups to forward multicast packets only to the multicast group member ports, thus avoiding wasting bandwidth by sending packets to ports that are not part of that multicast group. A switch that does not support IGMP or IGMP Snooping can not tell multicast packets from broadcast packets, so it can only treat them all as broadcast packets. Without IGMP Snooping, the multicast packet forwarding function is essentially that used by broadcast packets.

This switch supports IGMP Snooping with the functions of query, report and leave, using a type of packet exchanged between an IP Multicast Router/Switch and an IP Multicast Host that can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

Fig. 3-22

Function name:

IGMP Snooping

Function description:

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either the passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member ports.

Parameter description:

IGMP snooping mode selection:

The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

Disable:

Set “Disable” mode to disable IGMP Snooping function.

Default: Disable

Active:

In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. This also reduces unnecessary multicast traffic.

Passive:

In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.

IP Address:

Shows all multicast groups IP addresses that are registered on this device.

VLAN ID:

Shows the VLAN ID for each multicast group.

Member Port:

Shows member ports that join each multicast group. A member port may be in only one or more than one group.

3-8. Max. Packet Length

Function name:

Max. Packet Length

Function description:

The switch is capable of dealing with 9k Jumbo Frames, which suits the transmission of large amounts of data in the network environment.

Parameter description:

Jumbo Frame (bytes):

Set up the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1518 bytes.

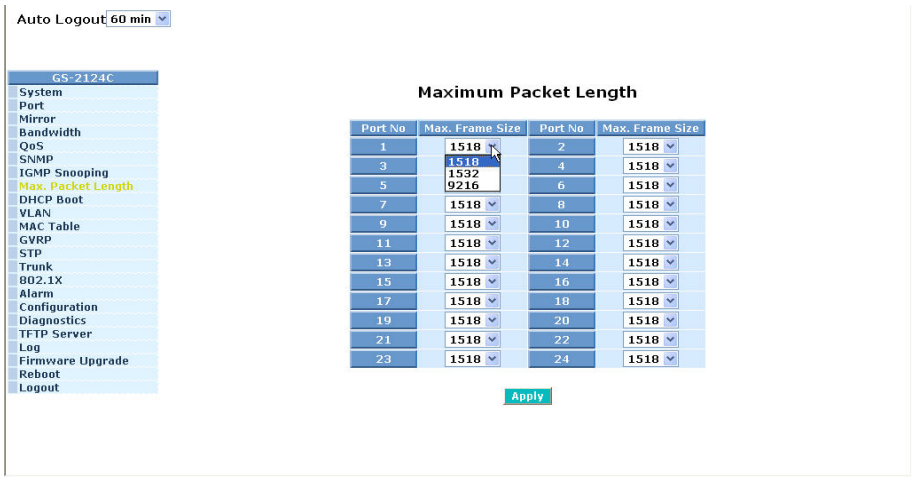


Fig. 3-23

3-9. DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a longer time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many predefined connections when the whole building or block loses electrical power and then attempts to reboot and recover. When an event like that occurs, a number of switches or other network devices on the LAN will try their best to find the server to get the services they require or try to set up the predefined links. In doing so, they will issue many broadcast packets in the network.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at the booting stage at the same time. The maximum user-defined delay time is 30 sec. If the DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exact delay time is computed by the switch itself. The default is “Disable”.

Fig. 3-24

3-10. VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. It supports 256 active VLANs, and VLAN IDs 1~4094. VLAN configuration is used to partition your LAN into small ones as your requirements demand. By properly configuring it, you can gain not only improved security and increased performance, but you can also greatly reduce VLAN management time.

3-10-1. VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes five modes: Port-based, Tag-based, Metro Mode, Double-tag and Disable. You can choose one of them by pulling down the list and pressing the **<Downward>** arrow key. Then, click the **<Apply>** button, and the settings will take effect immediately.

Parameter description:

VLAN Mode:

Disable:

Stops the VLAN function on the switch. In this mode, no VLAN is applied to the switch. This is the default setting.

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members ports 1 & 2 & 3 & 4. If you are on port 1, you can communicate with ports 2 & 3 & 4. If you are on port 5, then you cannot communicate with them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to a maximum of 24 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its members by VID. This is quite different from port-based VLAN. If there are any more rules in the ingress filtering list or the egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports a supplement of IEEE 802.1Q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned a VLAN name and a VLAN ID. Valid VLAN IDs are 1-4094. The user can create a total of up to 64 Tagged VLAN groups.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method of Port-based VLAN. It will create 22 or 23 Port-based VLAN groups.

Double-tag:

Double-tag mode belongs functionally to the tag-based mode; however, it would treat all frames as untagged, which means that a tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag packets.

Fig. 3-25

Uplink Port:

This function is enabled only when metro mode is chosen as the VLAN mode.

23:

Except Port 23, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 23, thus, total 23 groups consisting of 2 members are formed.

24:

Except Port 24, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 24, thus, total 23 groups consisting of 2 members are formed.

23 & 24:

Except Port 23 and Port 24, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 23 and Port 24, thus, total 22 groups consisting of 3 members are formed.

Fig. 3-26

3-10-2. Tag-based Group

Function name:

Tag-based Group Configuration

Function description:

Shows the information of existing Tag-based VLAN Groups. You can also easily create, edit and delete a Tag-based VLAN group by pressing the **<Add>**, **<Edit>,** and **<Delete>** function buttons. The user can add a new VLAN group by inputting a new VLAN name and VLAN ID.

Parameter description:

VLAN Name:

The name as defined by the administrator that is associated with a VLAN group. Valid characters are A-Z, a-z and 0-9. Other special characters will not be accepted. The maximum length is 15 characters.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

SYM-VLAN:

While the SYM-VLAN function of the group is enabled, all packets with this group VID will be dropped in case they are transmitted from the ports that do not belong to this group.

Member:

This is used to enable or disable a port's membership in a newly added VLAN. "Enable" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

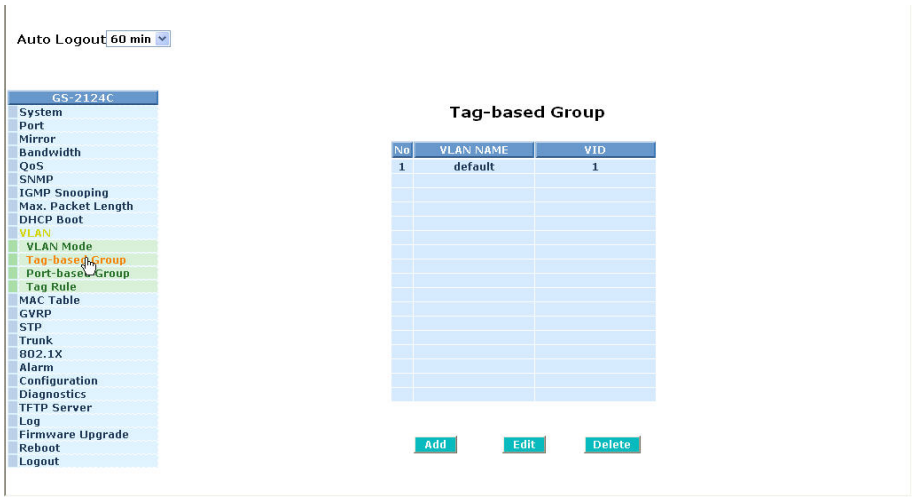


Fig. 3-27

Add Group:

Create a new Tag-based VLAN. Input the VLAN name as well as the VID, configure the SYM-VLAN function, and choose the member by ticking the check box beside the port number. Then press the **<Apply>** button to have the setting take effect.

Fig. 3-28

Delete Group:

Press the **<Delete>** button to remove the selected group entry from the Tag-based group table.

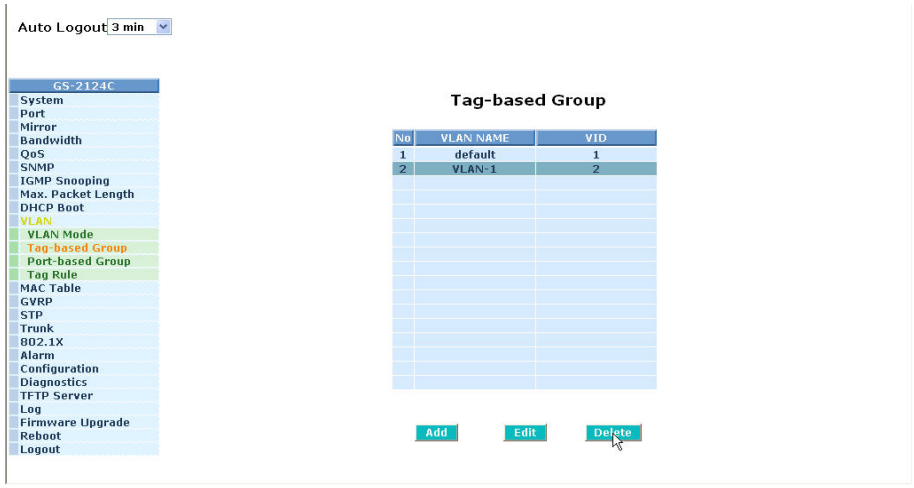


Fig. 3-29

Edit a group:

Select a group entry and press the **<Edit>** button; then you can modify a group's description, SYM-VLAN and member set.

3-10-3. Port-based Group

Function name:

Port-based Group Configuration

Function description:

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name.

Parameter description:

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letter is A-Z, a-z and 0-9. Other special characters will not be accepted. The maximal length is 15 characters.

Member:

This is used to enable or disable if a port is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Fig. 3-30

Add Group:

To create a new Port-based VLAN, input the VLAN name and choose the member by ticking the check box beside the port number. Then press the **<Apply>** button to have the setting take effect.

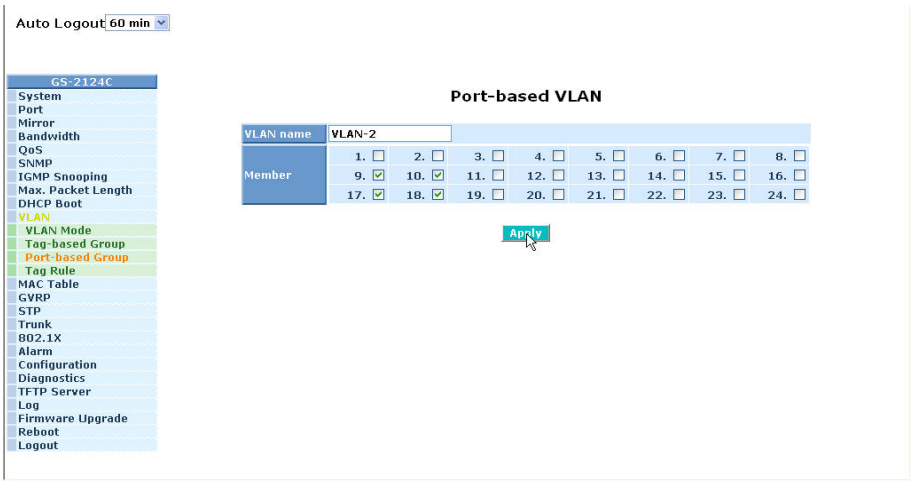


Fig. 3-31

Delete Group:

Press the **<Delete>** button to remove the selected group entry from the Port-based group table.

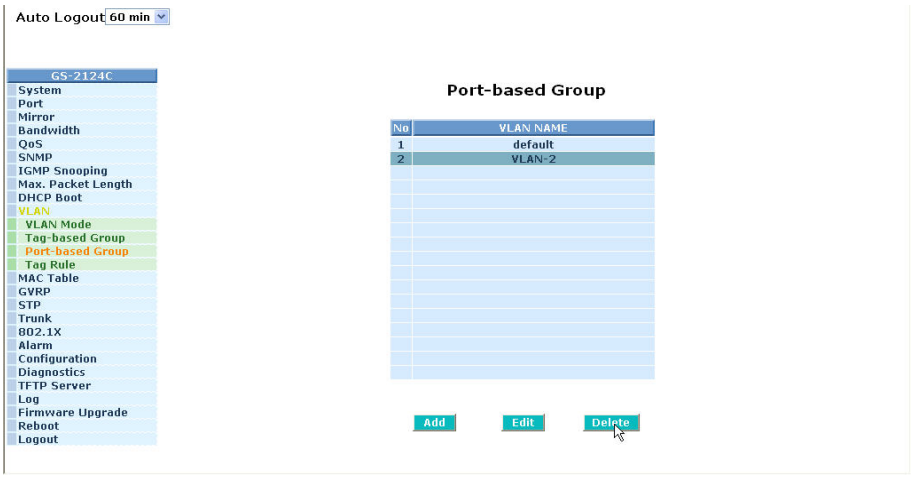


Fig. 3-32

Edit a group:

Select a group entry and press the **<Edit>** button; then you can modify a group‘s description and member set.

3-10-4. Tag Rule

Function name:

Tag Rule

Function description:

In VLAN Tag Rule Setting, the user can input the VID number to each port. The range of valid VID numbers is from 1 to 4094. The user also can choose ingress filtering rules for each port. There are two ingress filtering rules which can be applied to the switch. Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. Ingress Filtering Rule 2 is “drop untagged frame”. You can also assign the Role of each port as Access, Trunk, or Hybrid.

Parameter description:

Port 1-24:

Port number.

PVID:

The valid PVID range is 1-4094. Before a number x is set as a PVID, a Tag-based VLAN with VID x must be created. For example, if port x receives an untagged packet, the switch will apply the PVID (assumed in this example as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Rule 1:

Forward only packets with VID matching this port’s configured VID. Rule 1 can be applied as a way to use a given port to filter unwanted traffic. In Rule 1, a given port checks if the given port is a member of the VLAN on which the received packet belongs to, to determine whether to forward it or not. For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Rule 1 is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

Rule 2:

Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then both tagged and untagged packets will be processed. If the latter is the case, only the packets carrying a VLAN tag will be processed, and the rest of the packets will be discarded.

Note: If Rule 1 is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, and the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

Role:

This is an egress rule of the port. Valid Roles are termed Access, Trunk or Hybrid. Trunk means the outgoing packets must carry a VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. The Hybrid Role, is similar to the Trunk Role, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID:

Valid range is 0~4094. It works only when the Role is set to Hybrid.

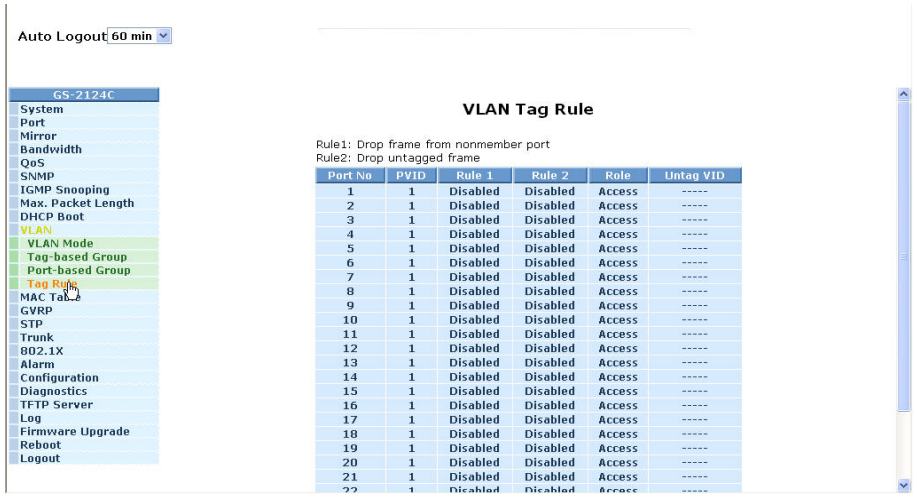

Auto Logout 60 min
GS-2124C
System
Port
Mirror
Bandwidth
QoS
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
VLAN Mode
Tag-based Group
Port-based Group
Tag Rule
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
VLAN Tag Rule
Rule1: Drop frame from nonmember port
Rule2: Drop untagged frame
Port No | PVID | Rule 1 | Rule 2 | Role | Untag VID
1 | 1 | Disabled | Disabled | Access | -----
2 | 1 | Disabled | Disabled | Access | -----
3 | 1 | Disabled | Disabled | Access | -----
4 | 1 | Disabled | Disabled | Access | -----
5 | 1 | Disabled | Disabled | Access | -----
6 | 1 | Disabled | Disabled | Access | -----
7 | 1 | Disabled | Disabled | Access | -----
8 | 1 | Disabled | Disabled | Access | -----
9 | 1 | Disabled | Disabled | Access | -----
10 | 1 | Disabled | Disabled | Access | -----
11 | 1 | Disabled | Disabled | Access | -----
12 | 1 | Disabled | Disabled | Access | -----
13 | 1 | Disabled | Disabled | Access | -----
14 | 1 | Disabled | Disabled | Access | -----
15 | 1 | Disabled | Disabled | Access | -----
16 | 1 | Disabled | Disabled | Access | -----
17 | 1 | Disabled | Disabled | Access | -----
18 | 1 | Disabled | Disabled | Access | -----
19 | 1 | Disabled | Disabled | Access | -----
20 | 1 | Disabled | Disabled | Access | -----
21 | 1 | Disabled | Disabled | Access | -----

Fig. 3-33

3-11. MAC Table

MAC Table Configuration contains many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type. They are described below.

Function name:

MAC Table Information

Function Description:

Displays the static or dynamic learning MAC entry and the state for the selected port.

Parameter description:

Port:

Selects the port about which you would like to inquire.

Search:

Sets up the MAC entry about which you would like to inquire.

The default is ??-??-??-??-??-??

MAC:

Displays the MAC address of one entry you selected from the searched MAC entries table.

Alias:

Sets up the Alias for the selected MAC entry.

Set Alias:

Saves the Alias of MAC entry you set up.

Search:

Find the entry that matches your setup.

Previous Page:

Moves to the previous page.

Next Page:

Moves to the next page.

Alias:

The Alias of the searched entry.

MAC Address:

The MAC address of the searched entry.

Port:

The port that exists in the searched MAC Entry.

VID:

The VLAN Group within which that MAC Entry exists.

State:

Displays the method that this MAC Entry is built to use. It may show “Dynamic MAC” or “Static MAC”.

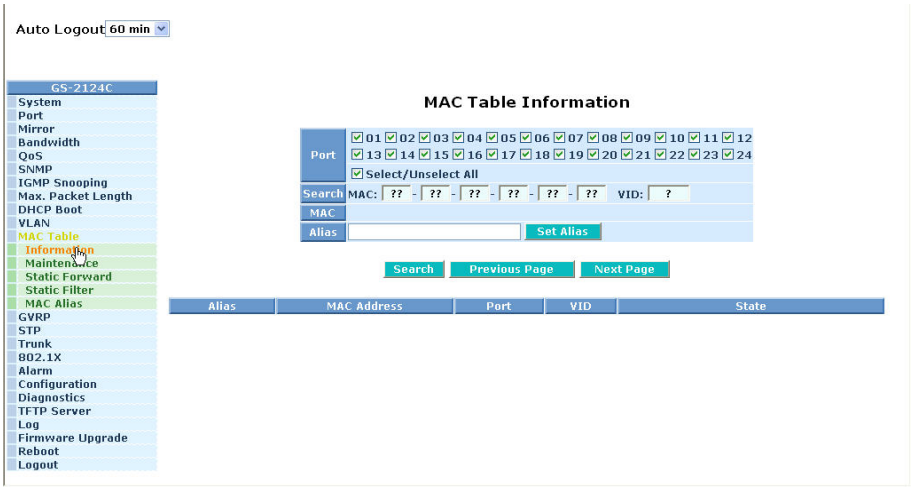


Fig. 3-34

Function Name:

MAC Table Maintenance

Function Description:

This function allows the user to set up the processing mechanism of the MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-800 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the user also has the right to decide enabling or disabling the “Stop learning while CPU is busy” function based upon the usage of the switch. This setup will influence the amount of packets flooding inside of the switch while the CPU is busy. The default age-out time is 300 seconds.

Parameter description:

Aging Time:

Deletes a MAC address idling for a period of time from the MAC Table, and will not affect static MAC address. Range of MAC Address Aging Time is 10-800 seconds. The default Aging Time is 300 seconds.

Flush:

Remove all entries that do not belong to the static MAC Entry from the MAC Table.

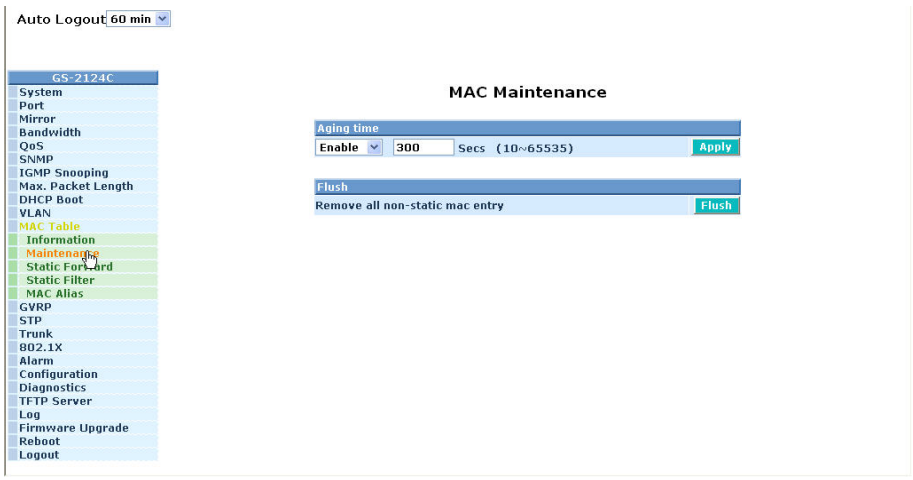


Fig. 3-35

Function Name:

Static Forward

Function Description:

Static Forward allows the user to access a specified port of the switch in the static forward table. The Static Forward table is associated with a specified port of a switch, and is set up by manually inputting the MAC address and its alias name.

When a MAC address is assigned to a specific port, all of the switch's traffic sent to this MAC address will be forwarded to this port.

For adding a MAC address entry in the allowed table, four parameters must be assigned: MAC address, associated port, VID and Alias. A MAC address entry can be removed by selecting the existing MAC address entry desired and clicking the **<Delete>** button.

Parameter description:

MAC:

Media Access Control address. A six-byte long Ethernet hardware address, usually expressed in hexadecimal ("hex') and separated by hyphens. For example:

00 – 40 - C7 - D6 – 00 - 01

Port No:

Port number of the switch. Valid range is 1 ~24.

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

MAC alias name; user-assigned.

Fig. 3-36

Function name:

Static Filter

Function Description:

Static Filter is a function that denies packet forwarding if the packet's MAC Address is listed in the Static Filter table. The user can maintain the table very easily by filling in the MAC Address, VID (VLAN ID) and Alias fields individually. The user also can delete an existing entry by clicking the **<Delete>** button.

Parameter description:

MAC:

Media Access Control address. A six-byte long Ethernet hardware address, usually expressed in hexadecimal ("hex') and separated by hyphens. For example:

00 – 40 - C7 - D6 – 00 - 01

Port No:

Port number of the switch. Valid range is 1 ~24.

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

MAC alias name; user-assigned.

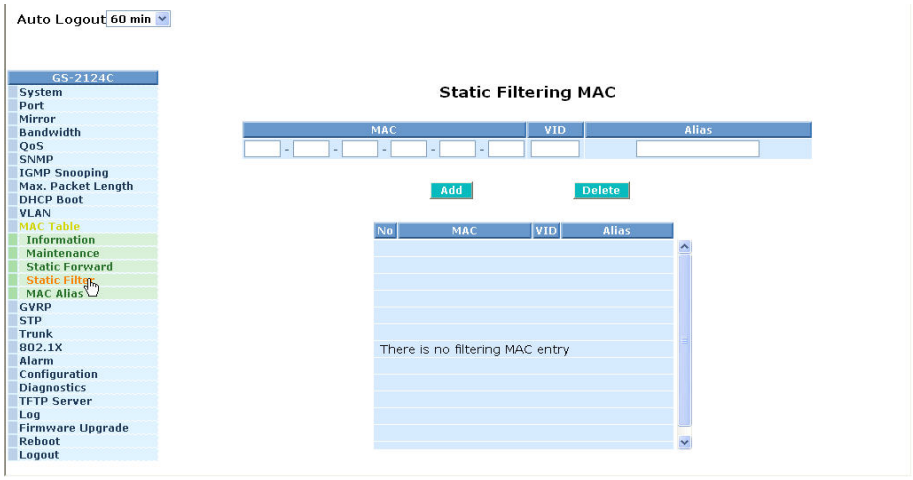


Fig. 3-37

Function name:

MAC Alias

Function description:

The MAC Alias function is used to let you assign a MAC address as a plain English name. This will help identify which MAC address belongs to which user in the illegal access report. Initially, it shows all pairs of the existing alias names and corresponding MAC addresses.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click the **<Create/Edit>** button to add/modify a new or an existing alias name for a specified MAC address, or mark an existing entry to delete it. An alias name must be composed of characters A-Z, a-z and 0-9 only and has a maximum length of 15 characters.

Function name:

MAC Alias Create/Edit or Delete

Function description:

Within the MAC Alias function, the MAC Alias Add/Edit function is used to add or modify an association between MAC address and a plain English name. User can click the **<Create/Edit>** button to add a new record with a MAC alias name.

The MAC Alias Delete function is used to remove an alias name from a MAC address. An existing MAC address or alias name can be selected for removal.

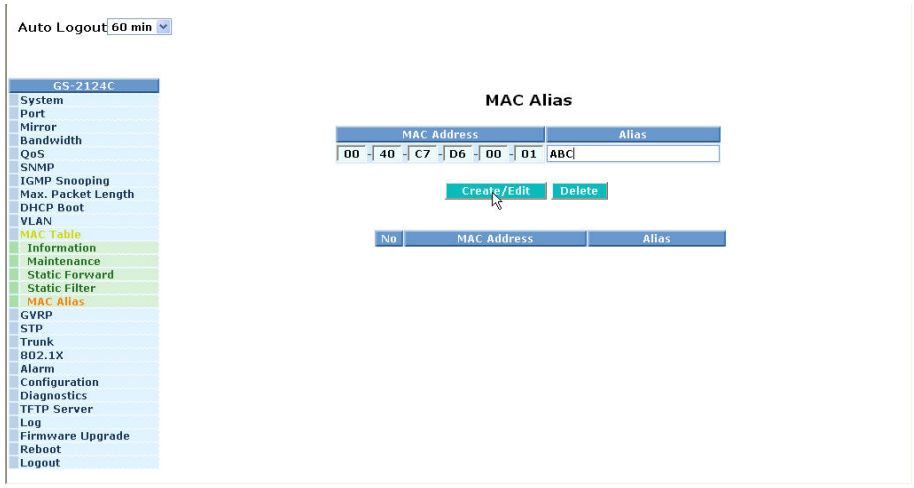


Fig. 3-38

Parameter description:

MAC:

Media Access Control address. A six-byte long Ethernet hardware address, usually expressed in hexadecimal (“hex’) and separated by hyphens. For example:

00 – 40 - C7 - D6 – 00 - 01

Alias:

MAC alias name; user-assigned.

Note: If there are many learned MAC addresses in the table, inputting the MAC address and alias name directly is recommended.

3-12. GVRP Configuration

GVRP is an application based on Generic Attribute Registration Protocol (GARP) that is primarily used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP provides the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, the GVRP state machine maintains the contents of Dynamic VLAN Registration Entries for each VLAN and propagates this information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and the ports through which these members can be reached.

In the GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter, and GVRP Group, as explained below.

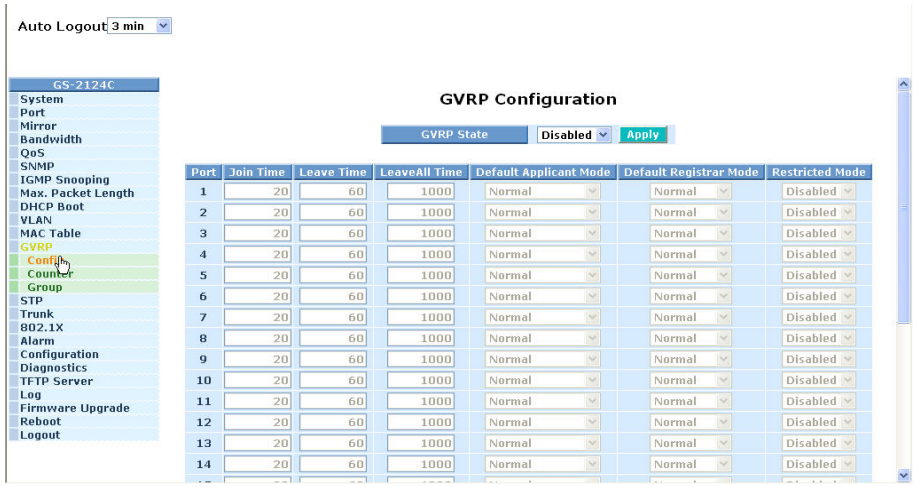


Fig. 3-39

Function name:

GVRP Config

Function description:

GVRP Config is used to configure each port's GVRP operation mode, in which there are seven parameters requiring configuration as described below.

Parameter description:

GVRP State Setting:

This function allows enabling or disabling of the GVRP function. To do this, pull down the list and click the **<Downward>** arrow key to choose "Enable" or "Disable", then click the **<Apply>** button; the new GVRP state will take effect immediately.

Join Time:

Used to declare the Join Time in units of centiseconds. Valid time range: 20 –100 centiseconds. Default: 20 centiseconds.

Leave Time:

Used to declare the Leave Time in units of centiseconds. Valid time range: 60 –300 centiseconds. Default: 60 centiseconds.

Leave All Time:

A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time. Default: 1000 unit time.

Default Applicant Mode:

This mode refers to the type of participant. There are two modes, normal participant and non-participant, that can be selected by the user.

Normal:

The participant is a Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

Non-Participant:

The participant is a Non-Participant. In this mode, the switch does not send or reply to any GARP messages. It listens to messages and only reacts to the received GVRP BPDU.

Default Registrar Mode:

This mode refers to the type of Registrar. There are three types of parameters for registrar administrative control value: normal registrar, fixed registrar, and forbidden registrar, that can be selected by the user.

Normal:

Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed:

Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden:

Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode:

This function is used to restrict creation of a dynamic VLAN when this port receives a GVRP PDU. There are two modes, disabled and enabled, that can be selected by the user.

Disabled:

In this mode, a dynamic VLAN will be created by the switch when this port receives a GVRP PDU. The default setting is Normal.

Enabled:

In this mode, the switch does not create a dynamic VLAN when this port receives a GVRP PDU. Except when the received dynamic VLAN message of the GVRP PDU is an existing static VLAN in the switch, this port will be added into the static VLAN members dynamically.

Function name:

GVRP Counter

Function description:

All GVRP counters are divided into two categories, Received and Transmitted. to let you monitor the GVRP actions. GVRP counters are actually GARP packets.

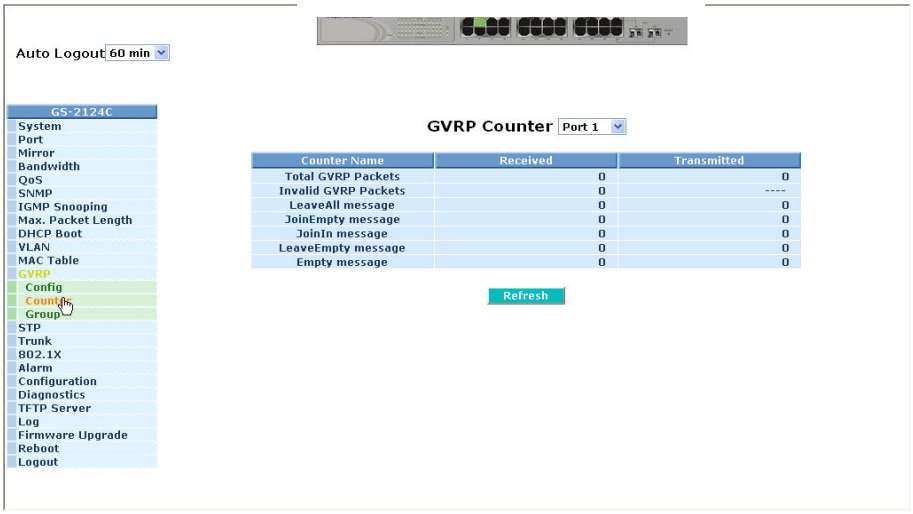


Fig. 3-40

Parameter description:

Received:

Total GVRP Packets:

Total GVRP BPDU packets received by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU packets received by the GARP application.

LeaveAll Message Packets:

Number of GARP BPDU packets with Leave All message received by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU packets with Join Empty message received by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU packets with Join In message received by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU packets with Leave Empty message received by the GARP application.

Empty Message Packets:

Number of GARP BPDU packets with Empty message received by the GARP application.

Transmitted:

Total GVRP Packets:

Total GARP BPDU packets transmitted by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU packets transmitted by the GVRP application.

LeaveAll Message Packets:

Number of GARP BPDU packets with Leave All message transmitted by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU packets with Join Empty message transmitted by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU packets with Join In message transmitted by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU packets with Leave Empty message transmitted by the GARP application.

Empty Message Packets:

Number of GARP BPDU packets with Empty message transmitted by the GARP application.

Function name:

GVRP Group Information

Function description:

Shows the dynamic group members and their information.

Parameter description:

VID:

VLAN identifier. When a GVRP group is created, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

Member Port:

Member ports belonging to the same dynamic VLAN group.

Edit Administrative Control:

When a GVRP group is created, the Administrative Control function is used to change the Applicant Mode and Registrar Mode of GVRP group members.

Refresh:

Provides the most current GVRP group status.

Fig. 3-41

3-13. STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, it ensures that only one path is active between any two nodes on the network at a time. The user can enable Spanning Tree Protocol via the switch's web management, and then set up other advanced items. Signamax recommends that STP be enabled on all switches to ensure a single active path between nodes on the network.

3-13-1. STP Status

Function name:

STP Status

Function description:

Spanning Tree Status addresses 12 parameters to provide the user with the current status of STP in the switch. The 12 parameters' descriptions are listed below.

Parameter description:

STP State:

Shows the current STP Enabled / Disabled status. Default is "Disabled".

Bridge ID:

Shows the switch's bridge ID, which stands for the MAC address of this switch.

Bridge Priority:

Shows this switch's current bridge priority setting. Default is 32768.

Designated Root:

Shows the root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.

Designated Priority:

Shows the current root bridge priority.

Root Port:

Shows the port number connected to the root bridge with the lowest path cost.

Root Path Cost:

Shows the path cost between the root port and the designated port of the root bridge.

Current Max. Age:

Shows the current root bridge maximum age time. Maximum age time is used to monitor and determine if the STP topology needs to change. When a bridge does not receive a hello message from the root bridge until the maximum age time has counted down to 0, the bridge will treat the root bridge as malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine what the root bridge is. Maximum Age time is assigned by the root bridge in units of seconds. Default is 20 seconds.

Current Forward Delay:

Shows the current root bridge forward delay time. The value of the Forward Delay time is set by the root. The Forward Delay time is defined as the time spent from the Listening state moved to the Learning state, or from the Learning state moved to the Forwarding state, of a port in a bridge.

Hello Time:

Shows the current hello time of the root bridge. Hello time is a time interval specified by the root bridge; it is used to request all other bridges to periodically sendia hello message every “hello time” seconds to the bridge attached to its designated port.

STP Topology Change Count:

STP Topology Change Count expresses the time spent in units of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but will be very close to that, because the time is constantly being eclipsed.

Time Since Last Topology Change:

Time Since Last Topology Change is the accumulated time in units of seconds the STP has been in effect since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. It will also begin counting again once the STP Topology Change is completed.

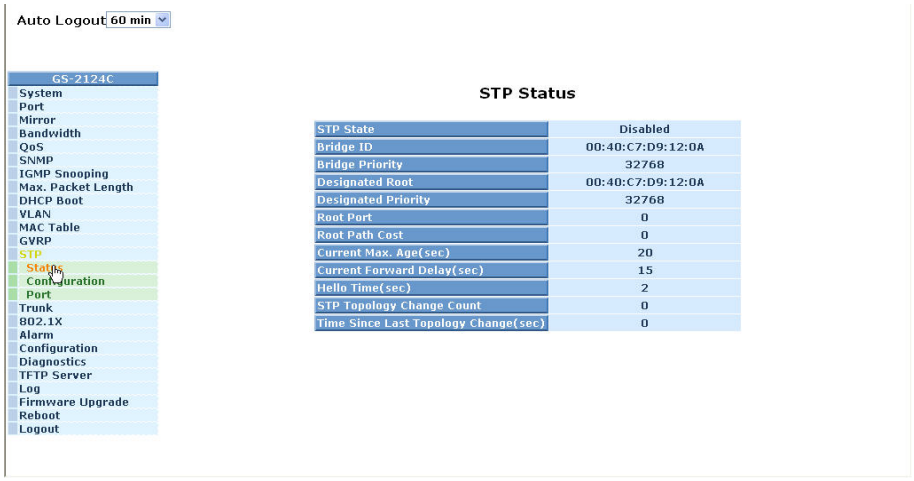


Fig. 3-42

3-13-2. STP Configuration

The STP, Spanning Tree Protocol, also includes Rapid Spanning Tree Protocol (RSTP). In the Spanning Tree Configuration, there are six parameters available for the user to configure as desired. Each parameter's description is listed below.

Function name:

STP Configuration

Function description:

The user can set the following Spanning Tree parameters to control the STP function, enable/disable, select mode RSTP/STP, and affect STP state machine behavior to send BPDU (Bridge Protocol Data Unit[1]) messages in this switch. The default setting of Spanning Tree Protocol is "Disable".

Parameter description:

Spanning Tree Protocol:

Sets the 802.1W Rapid STP function to "Enable" or "Disable". Default is "Disable"

Bridge Priority:

The lower the bridge priority number is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the 065-7840 managed switch as the root bridge, you can set this value lower than that of bridge in the LAN. The valid values are 0 ~ 61440. The default is 32768.

Hello Time:

Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to another bridge to tell it that it is alive. When the 065-7840 managed switch is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid values are 1 ~ 10, in units of seconds. Default is 2 seconds.

Max. Age:

When the 065-7840 managed switch is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originating from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge as malfunctioned, and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will recalculate and determine who the root bridge is. The valid values of Max. Age are 6 ~ 40 seconds. Default is 20 seconds.

[1] BPDUs are data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs, and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

Forward Delay:

The user can set the root bridge forward delay time. This figure is set only by the root bridge. The forward delay time is defined as the time spent from Listening state moved to Learning state, and also from Learning state moved to Forwarding state of a bridge port. The forward delay time contains two states: Listening state to Learning state, and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, and then the total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because of additional factors.

The valid values are 4 ~ 30 seconds, default is 15 seconds.

Force Version:

Two options are offered for the STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backwards compatible with STP (802.1d).

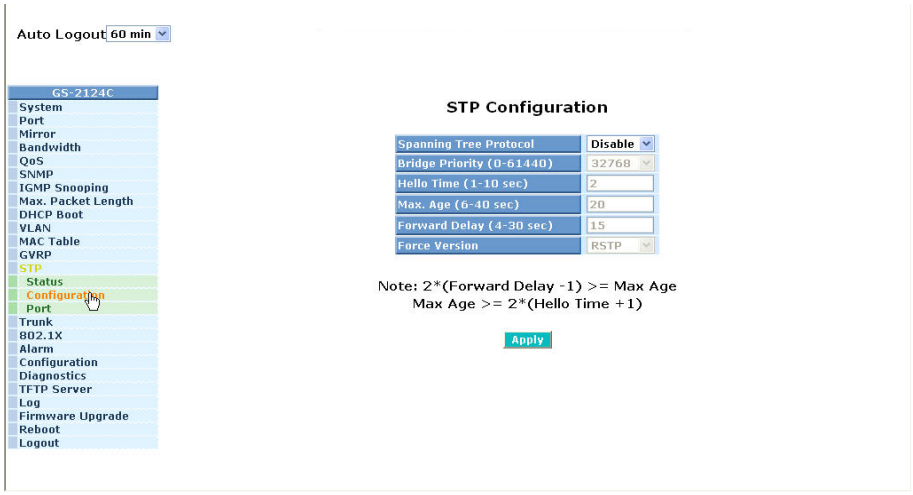


Fig. 3-43

3-13-3. STP Port Configuration

Function name:

STP Port Setting

Function description:

In the STP Port Setting, one item selection and five parameter settings are available for the user to configure as desired.. The user can disable and enable each port by selecting each Port Status item. The user also can set “Path Cost” and “Priority” of each port by filling in the desired value and set “Admin Edge Port” and “Admin Point To Point” by selecting the desired item.

Parameter description:

Port Status:

It displays the current state of a port. We cannot manually set it because it displays only the status. There are three possible states (according to the 802.1w specification):

- The DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

Notice: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

- The LEARNING state indicates this port can now contribute its learning knowledge but still cannot forward packets.

- The FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status:

Path Cost Status is the contribution value of the path through this port to the Root Bridge. The STP algorithm determines a best path to the Root Bridge by calculating the sum of the path costs contributed by all ports on this path. A port with a smaller path cost value would more probably become the Root Port.

Configured Path Cost:

The valid range is 0 – 200,000,000. In the switch, if the path cost is set to zero, the STP will get the recommended value resulting from auto-negotiation of the link accordingly and display this value in the Path Cost Status field. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP recommended values: (Valid range: 1 – 200,000,000)

10 Mbps : 2,000,000

100 Mbps: 200,000

1 Gbps : 20,000

Default: 0

Priority:

Priority, in this case, means Port Priority. Port Priority and Port Number are combined to form the Port ID. Port IDs are often compared to determine which port of a bridge would become the Root Port. The valid range is 0 – 240.

Default is 128.

Admin Edge Port:

If user selects “Yes”, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology remains unchanged. However, unlike the designate port or root port, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

Default: No

Admin Point To Point:

From the RSTP’s point of view, a port is a point-to-point link if it is in full-duplex mode but is a shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will allow the port to fast transit to the forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If this parameter is configured to be Auto, it means RSTP will use the duplex mode that resulted from the auto-negotiation. In today’s switched networks, most links are running in full-duplex mode. The result may be half-duplex, however; in this case, the port will not fast transit to the Forwarding state. If this parameter is set as True, the port is treated as a point-to-point link by RSTP and unconditionally transited to the Forwarding state. If the parameter is set as False, fast transition to the Forwarding state will not happen on this port.

Default: Auto

M Check:

Migration Check. It forces the port to send out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly act as an RSTP port. To send an RSTP BPDU from the port you specified, click the **<M Check>** button.

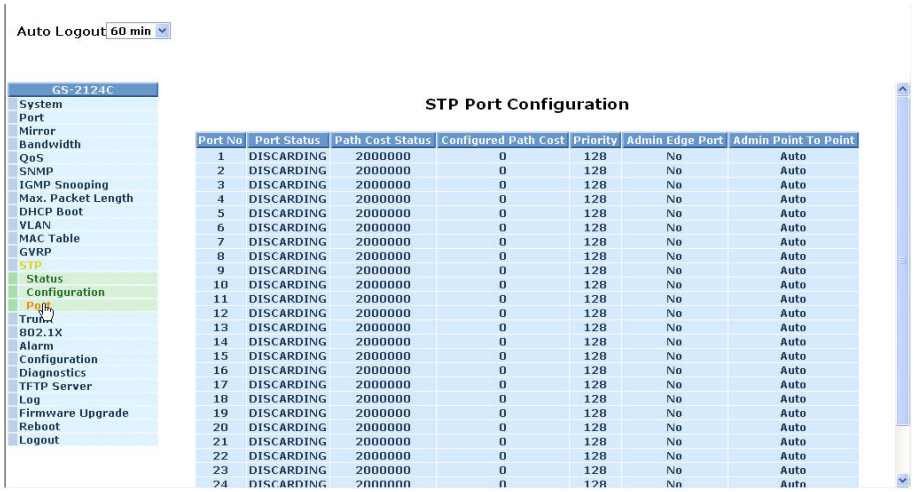

Auto Logout 60 min
GS-2124C
System
Port
Mirror
Bandwidth
QoS
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Status
Configuration
Port
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
STP Port Configuration
Port No | Port Status | Path Cost Status | Configured Path Cost | Priority | Admin Edge Port | Admin Point To Point
1 DISCARDING 2000000 0 128 No Auto
2 DISCARDING 2000000 0 128 No Auto
3 DISCARDING 2000000 0 128 No Auto
4 DISCARDING 2000000 0 128 No Auto
5 DISCARDING 2000000 0 128 No Auto
6 DISCARDING 2000000 0 128 No Auto
7 DISCARDING 2000000 0 128 No Auto
8 DISCARDING 2000000 0 128 No Auto
9 DISCARDING 2000000 0 128 No Auto
10 DISCARDING 2000000 0 128 No Auto
11 DISCARDING 2000000 0 128 No Auto
12 DISCARDING 2000000 0 128 No Auto
13 DISCARDING 2000000 0 128 No Auto
14 DISCARDING 2000000 0 128 No Auto
15 DISCARDING 2000000 0 128 No Auto
16 DISCARDING 2000000 0 128 No Auto
17 DISCARDING 2000000 0 128 No Auto
18 DISCARDING 2000000 0 128 No Auto
19 DISCARDING 2000000 0 128 No Auto
20 DISCARDING 2000000 0 128 No Auto
21 DISCARDING 2000000 0 128 No Auto
22 DISCARDING 2000000 0 128 No Auto
23 DISCARDING 2000000 0 128 No Auto
24 DISCARDING 2000000 0 128 No Auto

Fig. 3-44

3-14. Trunking Configuration

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as that of a single Fast Ethernet port.

The switch supports two kinds of port trunking methods:

LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~8) to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the following situations:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in the half-duplex mode
- Aggregating ports with different data rates

Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~8; this Static GroupID can be the same as another LACP groupID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both ends of a link is strongly recommended. Please also note that low speed links will stay in the “not ready” state when using Static Trunk to aggregate with high speed links.

There are system restrictions regarding the port aggregation function on the switch. From the management point of view, the switch supports a maximum of 8 trunk groups for LACP and an additional 8 trunk groups for Static Trunk. But in the system capability view, only 8 “real trunked” groups are supported. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

A Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

a) If 12 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the “None” trunking method and its Group ID will turn to 0. This means the port won’t aggregate with other ports.

b) If 14 ports all use LACP Trunk Group ID 1, a maximum of 12 ports can aggregate together and transit into the ready state.

c) A port using the “None“ trunking method or Group ID 0 will be automatically set to use the “None” trunking method with Group ID 0.

Function name:

Port Setting/Status

Function description:

Port setting/status is used to configure the trunk property of each and every port in the switch system.

Parameter description:

Method:

This determines the method a port uses to aggregate with other ports.

None:

A port the user does not want to aggregate with any other port should have this default setting chosen.

LACP:

A port using LACP as its trunk method, to allow aggregation with other ports that are also using LACP.

Static:

A port using Static Trunk as its trunk method, to allow aggregation with other ports that are also using Static Trunk.

Group:

Ports having the same trunking method chosen (other than “None”) must be assigned a unique Group number (i.e. Group ID; valid values are from 1 to 8) in order to declare that they are to aggregate with each other.

Active LACP:

This field is only referenced when a port’s trunking method is LACP.

Active:

An Active LACP port begins to send LACPDU (Link Aggregation Control Protocol Data Unit) to its link partner right after the LACP protocol entity started to take control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

Aggtr:

Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using the same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status:

This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---“ means “not ready”

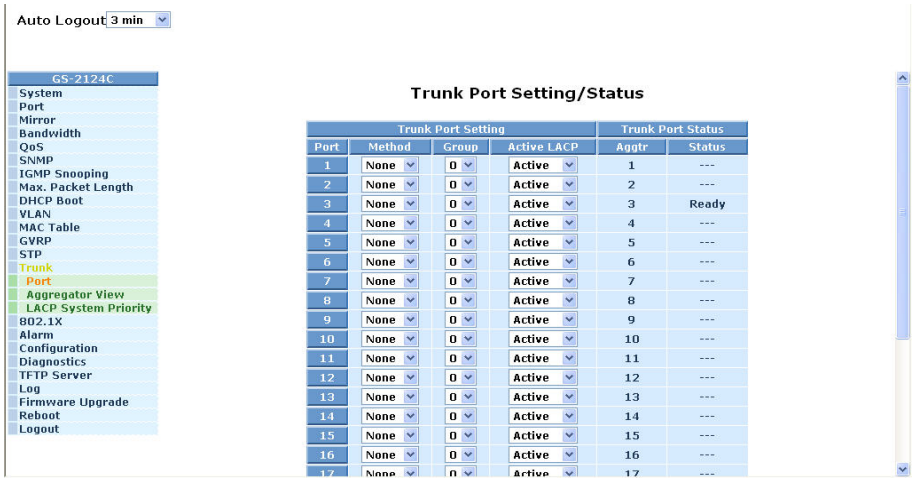


Fig.3-45

Function name:

Aggregator View

Function description:

To display the current port trunking information from the aggregator point of view.

Parameter description:

Aggregator:

Shows the aggregator ID (from 1 to 24) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

Method:

Shows the method a port uses to aggregate with other ports.

Member Ports:

Shows all member ports of an aggregator (port).

Ready Ports:

Shows only the ready member ports within an aggregator (port).

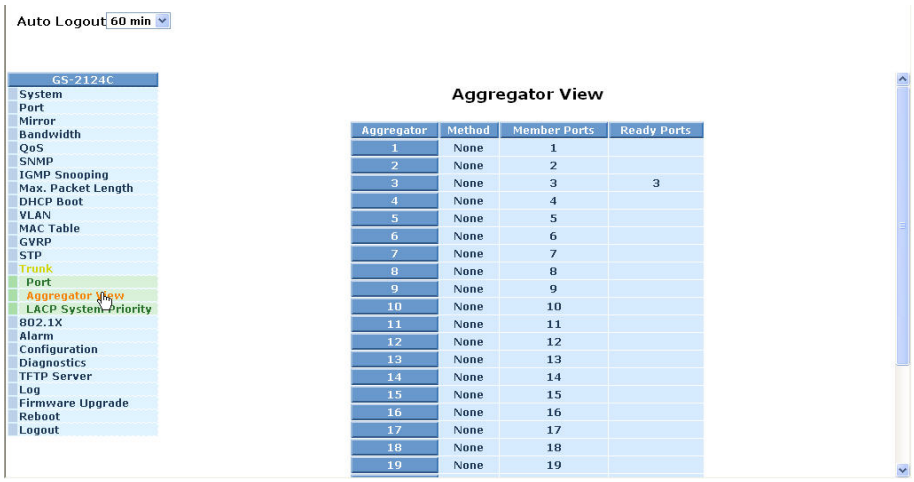


Fig.3-46

Function name:

LACP Detail (LACP Aggregator Detailed Information)

Function description:

Shows the detailed information of the LACP trunking group.

Parameter description:

Actor:

The switch you are observing.

Partner:

The peer system from this aggregator's view.

System Priority:

Shows the System Priority part of a system ID.

MAC Address:

Shows the MAC Address part of a system ID.

Port:

Shows the port number part of an LACP port ID.

Key:

Shows the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through switch management.

Trunk Status:

Shows the trunk status of a single member port."---" means "not ready"

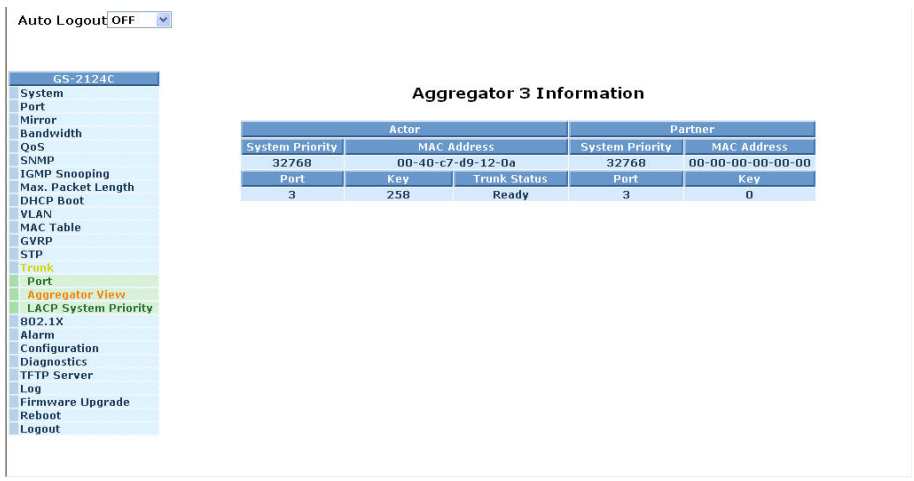


Fig. 4-47

Function name:

LACP System Priority

Function description:

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system that supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set by the user. Its valid range is from 1 to 65535. Default: 32768

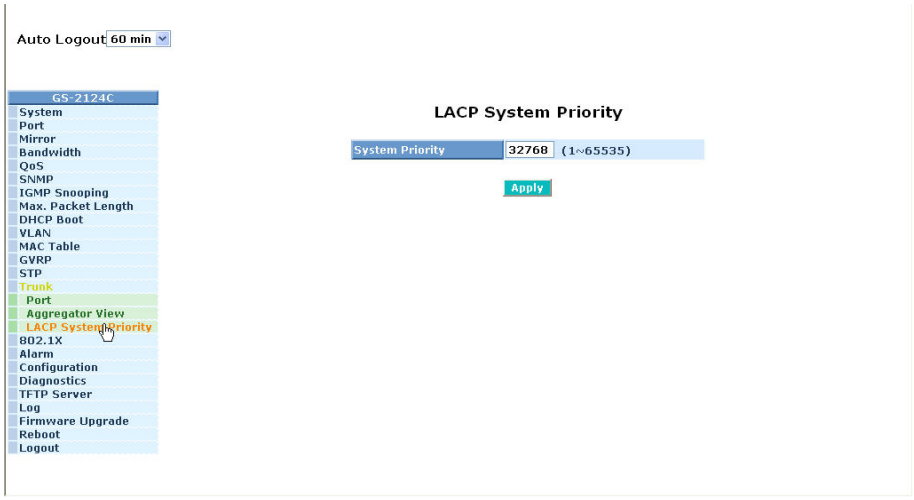


Fig.3-48

3-15. 802.1x Configuration

802.1x port-based network access control provides a method to restrict users to accessing network resources via authenticating the user's information. This restricts users from gaining access to the network resources through an 802.1x-enabled port without authentication. If a user wishes to administer the network through a port under 802.1x control, he or she must first input his or her account name for authentication and wait to receive authorization before sending or receiving any packets from an 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator; the authenticator passes the request to the authentication server to authenticate and verify, and the server tells the authenticator if the request has been granted authorization for the ports.

According to IEEE 802.1x, there are three components implemented. They are Authenticator, Supplicant, and Authentication server, as shown in Fig. 3-49.

Supplicant:

An entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE issues a request to it.

Authenticator:

An entity that facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of the authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once re-authentication of the supplicant has started, the controlled port remains in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with the PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by a MAC bridge, at any time.

Authentication server:

A device that provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow shown in Fig. 3-49 is quite simple. When the Supplicant PAE issues a request to the Authenticator PAE, the Authenticator and Supplicant exchange an authentication message. Then, the Authenticator passes the request to the RADIUS server for verification. Finally, the RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only contact the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

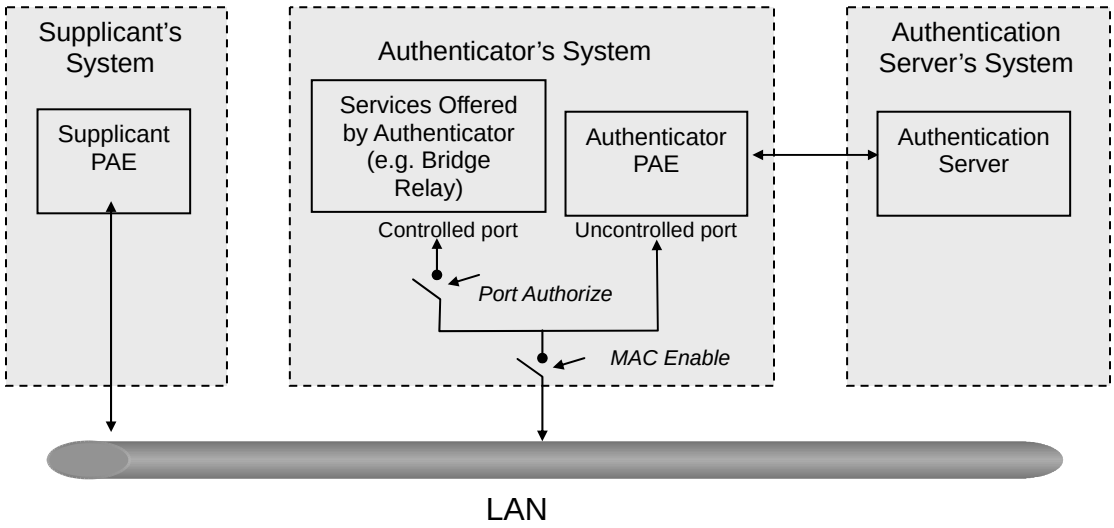


Fig. 3-49

Fig. 3-50 shows a typical configuration: a single supplicant, an authenticator and an authentication server. B and C are on the internal network, D is the Authentication server running RADIUS, the switch at the central location acts as the Authenticator connecting to PC A ,and A is a PC outside the controlled port, running Supplicant PAE. In this case, if PC A wants to access the services on devices B and C, it must first exchange the authentication message with the authenticator on the port on which it is connected via an EAPOL packet. The authenticator transfers the supplicant's credentials to the Authentication server for verification. If successful, the authentication server will notify the authenticator that access is granted. PC A is then allowed to access B and C via the switch. If there are two switches directly connected together instead of a single one, for the link connecting two switches, it may have to act in two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

Fig. 3-50

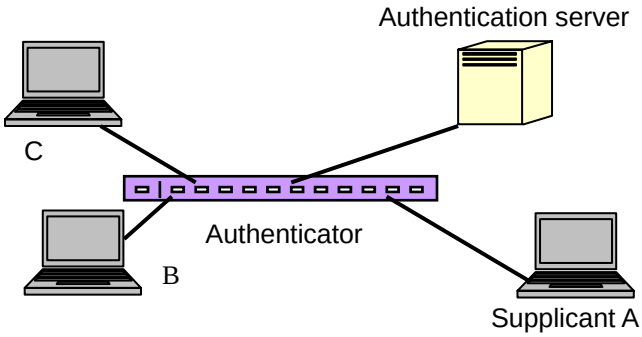


Fig. 3-51 shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on the switch acting as an authenticator is in an unauthorized state. Therefore, the access is blocked at this stage.

2. Initiating a session: Either the authenticator or the supplicant can initiate the message exchange. If the supplicant initiates the process, it sends an EAPOL-start packet to the authenticator PAE and the authenticator will immediately respond with an EAP-Request/Identity packet.

3. The authenticator always periodically sends EAP-Request/Identity to the supplicant in order to request the identity it wants to be authenticated.

4. If the authenticator doesn't send an EAP-Request/Identity, the supplicant will initiate the process by sending EAPOL-Start to the authenticator.

5. Next, the Supplicant replies with an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into a Radius-Access-Request command and send it to the authentication server for confirmation of its identity.

6. After receiving the Radius-Access-Request, the authentication server sends a Radius-Access-Challenge to the supplicant to ask for the input of the user password via the authenticator PAE.

7. The supplicant will convert the user password into the credential information in MD5 format and replies with an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to the authentication server via the authenticator PAE. As determined by the value of the type field in the message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, either EAP-MD5 (Message Digest 5), or EAP-OTP (One Time Password), or another type of algorithm.

8. If the user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant has failed to authenticate. The port to which it is connected is in the unauthorized state, and the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issue an EAP-Logoff message to Authentication server, the port used by the supplicant is set to be unauthorized.

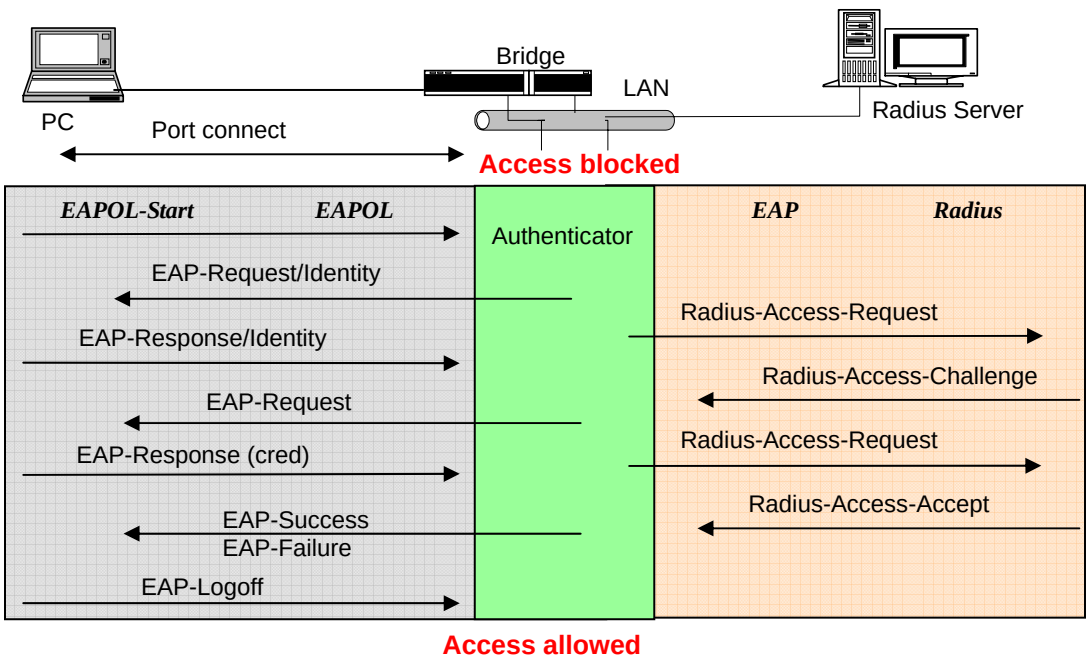


Fig. 3-51

Multihost 802.1X is the only type of authentication supported in the switch. In this mode, for the devices connected to this port, those devices can access the network resource through this port once a supplicant is authorized.

802.1x Port-based Network Access Control function supported by the switch is somewhat complex, for it just supports the basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode set in 802.1x Port mode, port control state, and as set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

Table 3-3

Function name:

802.1x State Setting

Function description:

This function is used to configure the global parameters for RADIUS authentication in the 802.1x port security application.

Parameter description:

Radius Server:

RADIUS server IP address for authentication.

Default: 192.168.1.1

Port Number:

The port number used to communicate with the RADIUS server for the authentication service. The valid value ranges from 1-65535.

Default port number is 1812.

Secret Key:

The secret key between the authentication server and the authenticator. It is a string with a length of 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is case-sensitive. Use of a blank between any two characters is not allowed.

Default: Radius

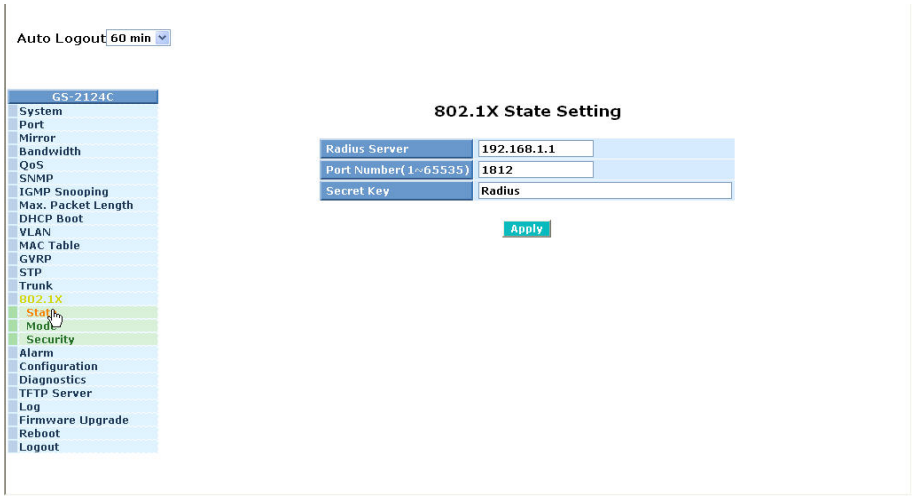


Fig. 3-52

Function name:

802.1x Mode Setting

Function description:

Sets the operation mode of 802.1X for each port. In this device, it supports only the Multihost operation mode.

Parameter description:

Port Number:

Indicates which port is selected to configure the 802.1x operation mode.

802.1x Mode:

802.1x operation mode. There are two options, Disable and Multihost mode. Default is "Disable".

- Disable

The chosen port acts as a plain port; that is, no 802.1x port access control works on the port.

- 802.1x with Multi-host

In this mode, for the devices connected to this port, those devices can access the network resource through this port once a supplicant is authorized.

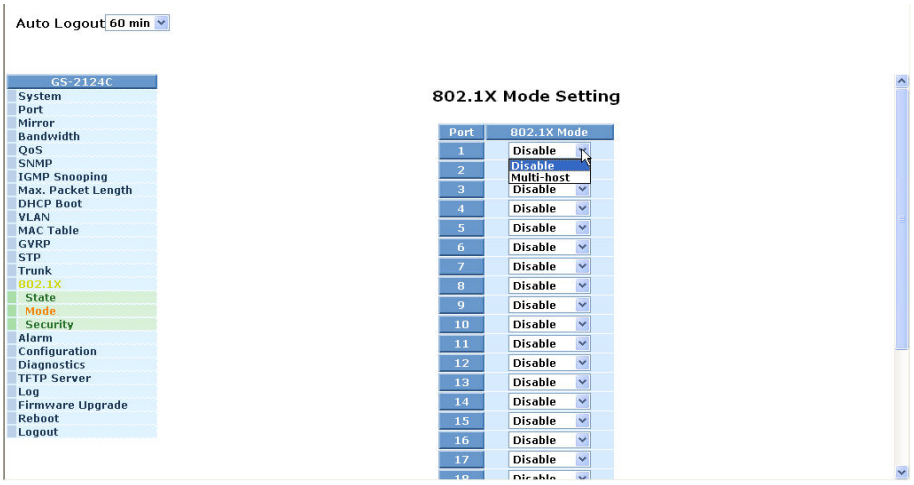


Fig. 3-53

Function name:

Port Security Management

Function description:

Shows each port status. In Multihost mode, it shows the port number and its status, authorized or unauthorized.

Parameter description:

Disable Mode:

When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply the 802.1X authenticator to it. Any node attached on this port can access the network without the permission of the 802.1X authenticator. The Port Status will show the following screen.

Port Number:

The port number to be chosen to show its 802.1X Port Status. The valid range of port numbers is Port 1 – 24.

Port Status:

The current 802.1X status of the port. In Disable mode, this field is Disabled.

802.1x with Multihost mode:

When selecting 802.1x with Multihost mode for a port in the function 802.1X Port Mode Configuration, Devices can access the network through this port once the authenticator is authorized. The Port Status will show the following screen. If the port is granted access to the network, the port status is authorized; otherwise, the port status is

Fig. 3-54

Function name:

Param. Setting

Function description:

Used to configure the parameters for each port in the 802.1x port security application. Refer to the following parameters' descriptions for details.

Parameter description:

Port:

The port number to be selected for configuring its associated 802.1x parameters, which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

Port Control:

This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

- ForceUnauthorized:

  The controlled port is forced to hold in the unauthorized state.

- ForceAuthorized:

  The controlled port is forced to hold in the authorized state.

- Auto:

  The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

  Default: Auto

reAuthMax(1-10):

The number of authentication attempts that are permitted before the port becomes unauthorized.

Default: 2

txPeriod(1-65535 s):

A time period to transmit EAPOL PDU between the authenticator and the supplicant.

Default: 30 seconds

Quiet Period(0-65535 s):

A period of time during which the switch will not attempt to access the supplicant.

Default: 60 seconds

reAuthEnabled:

Choose whether regular authentication will take place on this port.

Default: ON

reAuthPeriod(1-65535 s):

A non-zero number of seconds between the periodic re-authentication of the supplicant.

Default: 3600 seconds

max. Request(1-10):

The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. Valid range: 1 – 10.

Default: 2 times

suppTimeout(1-65535 s):

A timeout condition in the exchange between the authenticator and the supplicant. Valid range: 1 –65535.

Default: 30 seconds.

serverTimeout(1-65535 s):

A timeout condition in the exchange between the authenticator and the authentication server. Valid range: 1 –65535.

Default: 30 seconds

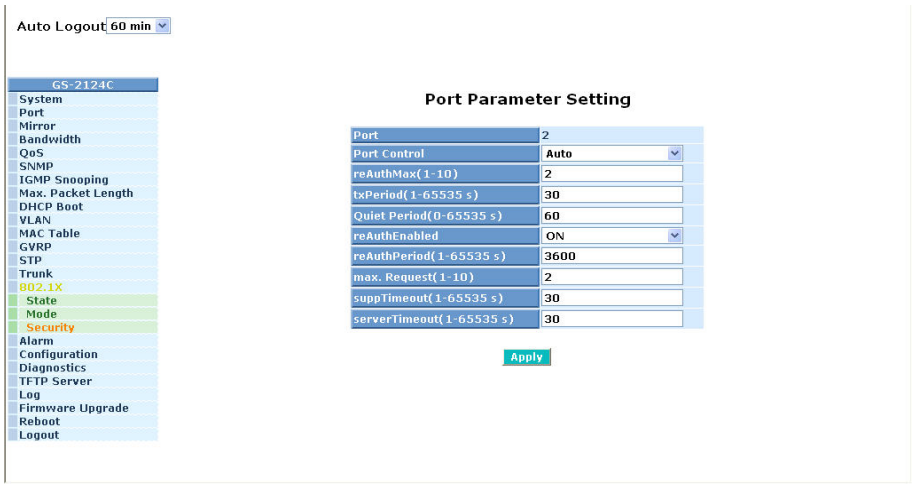
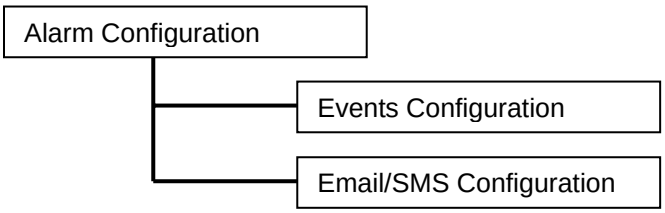


Fig. 3-55

3-16. Alarm Configuration



Function name:

Events Configuration

Function description:

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events have occurred. The switch offers 24 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (☑) the trap event individually on the web page shown as below.

Parameter description:

These trap functions are as they describe. The special one is Module Swap. It means that when the switch detects a module with the different module ID to be inserted, the switch treats it as Module swapped. The traps that the switch supports are listed below.

STP: STP Topology Change, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure

GVRP: GVRP Disabled, GVRP Enabled

VLAN: VLAN Disabled, Port-based VLAN Enable, Tag-based VLAN Enable, Metro-mode VLAN Enabled, Double-tag VLAN Enabled

Module Swap: SEP Inserted, SEP Removed, Dual-media Swapped

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

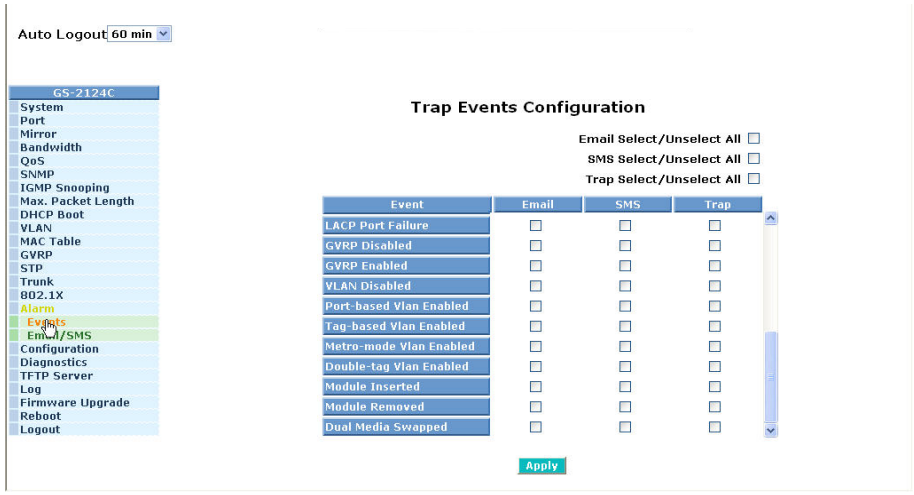


Fig. 3-56

Function name:

Email/SMS Configuration

Function description:

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both, depending on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration (See Fig. 3-57). The user can then read the trap information from the email or the mobile phone. This function provides a maximum of 6 email addresses and 6 mobile phone numbers. The 24 different trap events will be sent out to the SNMP Manager when the trap event occurs. After ticking trap events, the user can fill in the desired email addresses and mobile phone numbers. Clicking the **<Apply>** button completes the alarm configuration. It will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.

Parameter description:

Email:

Mail Server: The IP address of the server transferring your email.

Username: The desired username on the mail server.

Password: The password associated with the desired username on the mail server.

Email Address 1 – 6: Destination email address(es) for the alarm message.

SMS:

SMS Server: the IP address of the server transferring your SMS.

Username: The username in the ISP.

Password: The username in the ISP.

Mobile Phone 1-6: The destination mobile phone number(s) for the alarm message.

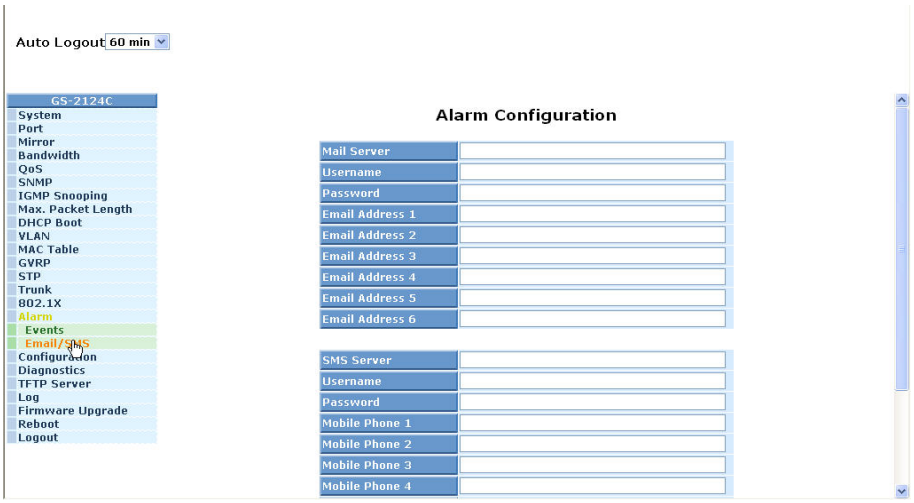


Fig. 3-57

3-17. Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

- **Default Configuration:**

  This is the setting as shipped from the factory; it cannot be altered.

- **Working Configuration:**

  This is the configuration you are using currently; it can be changed at any time. The configurations you are using are saved into this configuration file. This file is updated each time the **<Apply>** button is pressed.

- **User Configuration:**

  This is the configuration file specified for backup purposes; it can be updated by confirming the new configuration. You can retrieve it by performing the Restore User Configuration operation.

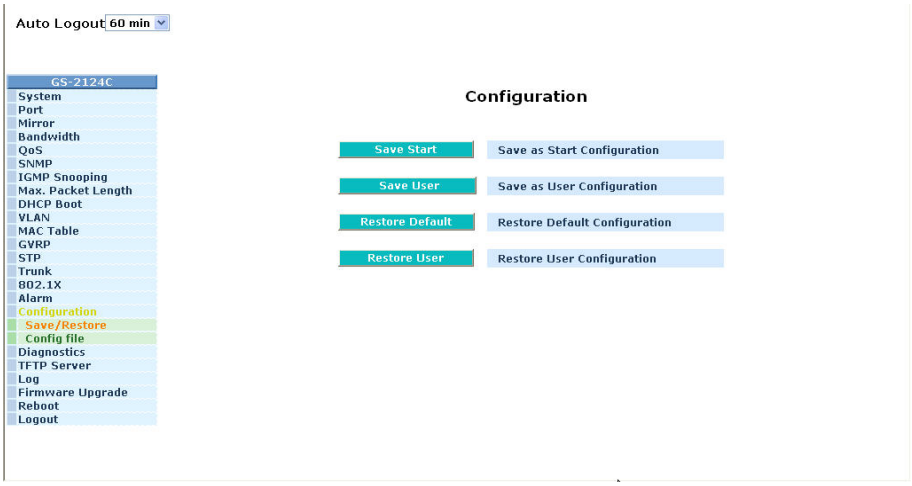


Fig. 3-58

3-17-1. Save/Restore

Function name:

Save As Start Configuration

Function description:

Saves the current configuration as a start configuration file in flash memory.

Fig. 3-59

Function name:

Save As User Configuration

Function description:

Saves the current configuration as a user configuration file in flash memory.

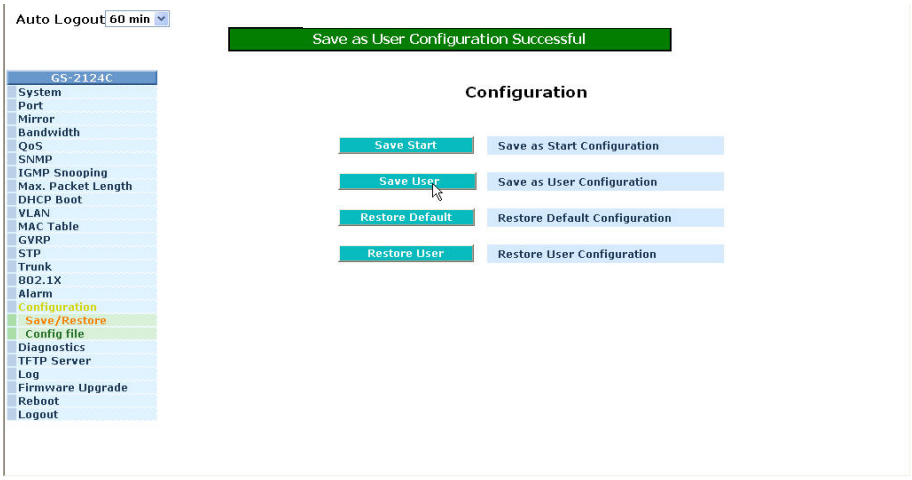


Fig. 3-60

Function name:

Restore Default Configuration

Function description:

Restore Default Configuration function retrieve the default factory settings to replace the start configuration.

Fig. 3-61

Function name:

Restore User Configuration

Function description:

Restore User Configuration function retrieves the previous confirmed working configuration stored in the flash memory to update the start configuration. When completing restoration of the configuration, the system's start configuration is updated and will change its system settings after rebooting the

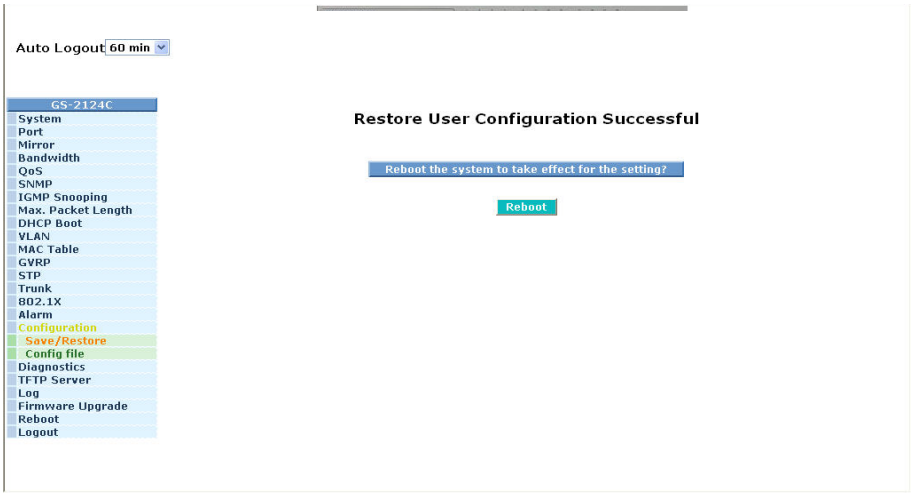


Fig. 3-62

3-17-2. Config File

Function name:

Config File

Function description:

This function is used to back up or reload the configuration files of Save As Start or Save As User via TFTP.

Parameter description:

Export File Path:

Export Start:

Export the Save As Start's configuration file stored in the flash memory.

Export User-Conf:

Export the Save As User's configuration file stored in the flash memory.

Import File Path:

Import Start:

Import the Save As Start's configuration file stored in the flash memory.

Import User-Conf:

Import the Save As User's configuration file stored in the flash memory.

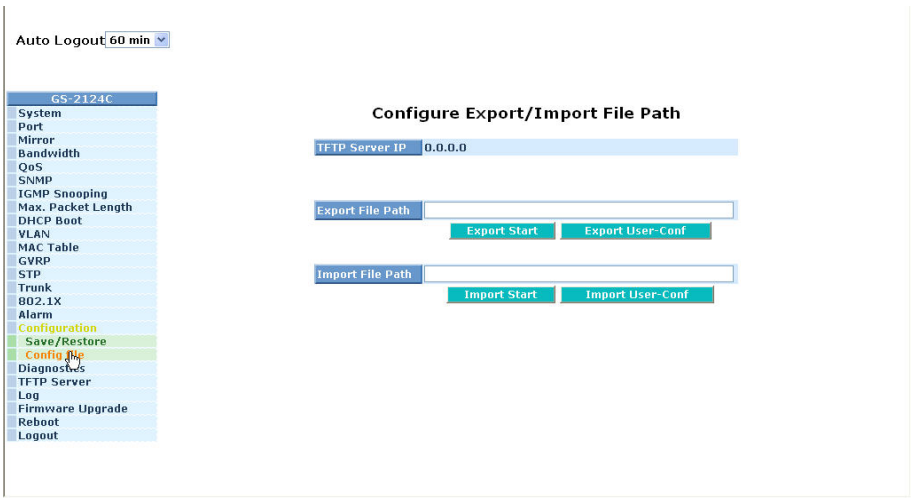
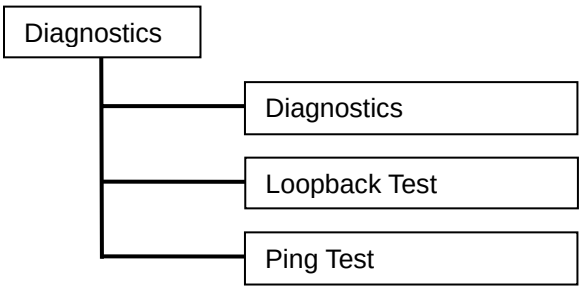


Fig. 3-63

3-18. Diagnostics

Three functions, Diagnostics, Loopback Test and Ping Test, are contained in this function folder for device self-diagnostics. Each of them will be described in detail in the following sections.



Function name:

Diagnostics

Function description:

This function provides a set of basic system diagnostics that allows the user to check the health of the system. The basic system check includes the EEPROM test, the UART test, the DRAM test, and the Flash test

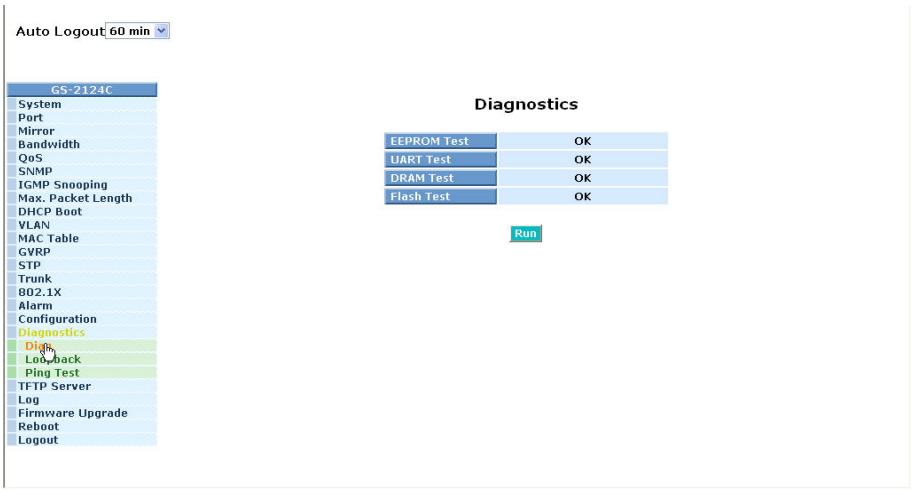


Fig. 3-64

Function name:

Loopback Test

Function description:

There are two different loopback tests included within the Loopback Test function: the Internal Loopback Test and the External Loopback Test. The Internal Loopback Test will not send the test signal outside the switch box. The test signal only wraps around within the switch box. The External Loopback Test will send the test signal to its link partner. If the switch is not connected to active network devices, i.e. the ports are link down, the switch will report those port numbers as failed. The test shows OK on a port when that port is linked.

Note: The Loopback Tests are disruptive tests. Whether you choose the Internal Loopback Test or the External Loopback Test, these two functions will interfere with the normal system operation; sending and receiving of all packets will stop for the duration of the test.

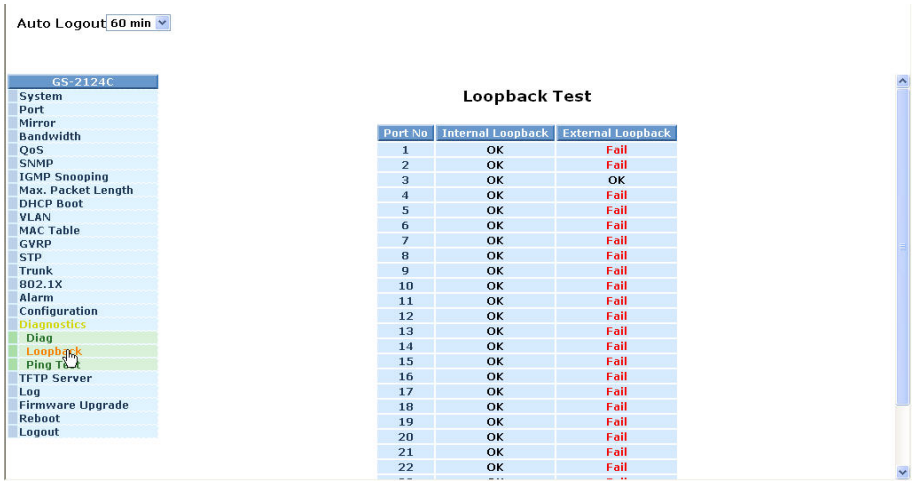


Fig. 3-65

Function name:

Ping Test

Function description:

The Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol, which abounds with report messages that can tell the user if the target device is available or not. The user fills in a known IP address and then click **<Ping>** button. A few seconds later, the switch will report if the pinged device is alive or dead in the Ping Result field.

Parameter description:

IP Address:

An IP address with the version of v4, e.g. 192.168.1.1.

Default Gateway:

IP address of the default gateway.

For more details, please see the section relating to IP addresses in Chapter 2.

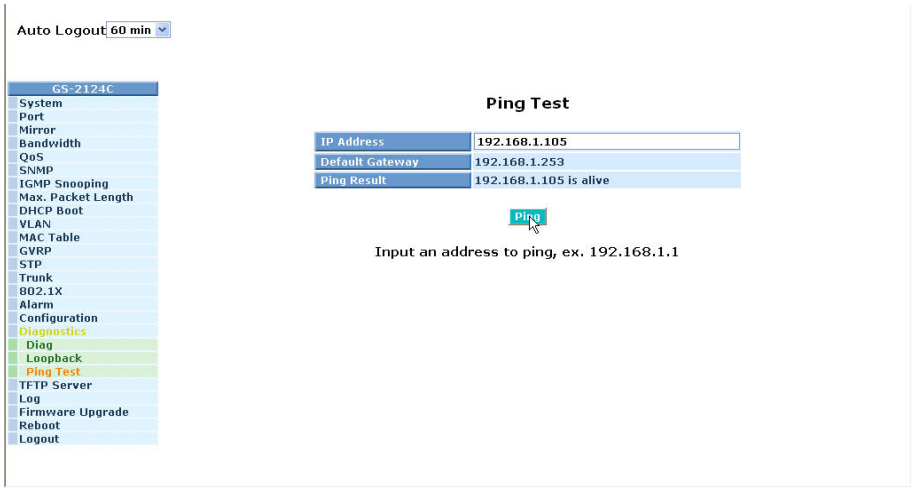


Fig. 3-66

3-19. TFTP Server

Function name:

TFTP Server

Function description:

Sets up the IP address of a TFTP server.

Parameter description:

Specify the IP address where the TFTP server is located by filling in the IP address field; then press the **<Apply>** button to have the setting take effect.

Fig. 3-67

3-20. Log

This function shows the log data. The switch provides system log data for users. There are 19 private trap logs, and 5 public trap logs. The switch supports a total of 120 log entries. For more details on log items, please refer to the section of this manual relating to Trap/Alarm Configuration and SNMP Configuration.

Function name:

Log Data

Function description:

The Trap Log Data displays the log items, including all SNMP Private Trap events, SNMP Public traps, and user logs that have occurred in the system. In the report table, No., Time, and Events are three fields contained in each trap record.

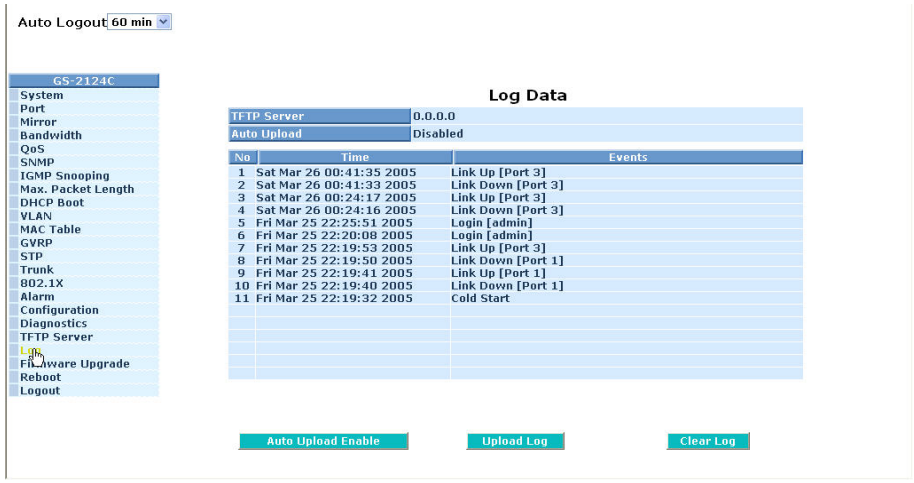


Fig. 3-68

Parameter description:

No.:

Displays the number in the order that the trap occurred.

Time:

Displays the time that the trap occurred.

Events:

Displays the trap event name.

Auto Upload Enable:

Switches the enabled or disabled status of the auto upload function.

Upload Log:

Uploads the log data through TFTP.

Clear Log:

Clears the log data.

3-21. Firmware Upgrade

A software upgrade tool is used to help upgrade the software in order to fix or improve the switch's functionality. The switch provides a TFTP client for software upgrades. This can be done using an Ethernet connection.

Function name:

Firmware Upgrade

Function description:

The switch supports a TFTP upgrade tool for upgrading its software. If the user desires upgrading the switch's software to a newer version, two procedures must be followed:

1.) Specifying the IP address where the TFTP server is located. The IP address of your TFTP server should be entered in this field.

2.) Specifying what the filename is and where the file is located. You must specify the full path and filename.

Once you press the **<Upgrade>** button, the switch will prompt the user to reconfirm. The switch then begins downloading the software from the TFTP server if the **<OK>** button is chosen. The switch will revert back to "Software Upgrade" if you choose the **<Cancel>** button.

If the download is not successful, the switch will also revert back to "Software Upgrade", and it will not upgrade the software.

When the download is completed, the switch begins upgrading its software. A reboot prompt message will be displayed after completing the software upgrade. At this time, you must reboot the switch to have the new software take effect.

Note: Upgrading the software is hazardous if the power is off. It must be done carefully.

Parameter description:

TFTP Server: A TFTP server stored the image file you want to upgrade.
Path and Filename: File path and filename stored the image file you want to upgrade.

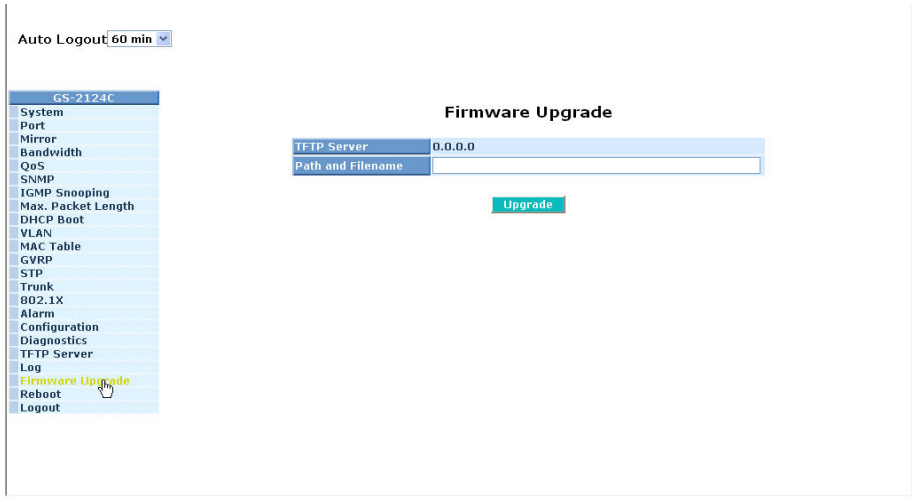


Fig. 3-69

3-22. Reboot

The user has many ways to reboot the switch, including power up, hardware reset and software reset. Pressing the RESET button in the front panel resets the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, the switch must be rebooted to have the new configuration take effect. The function discussed here provides a software reset for the “reboot” in the main menu.

Function name:

Reboot

Function description:

Reboots the switch. Reboot has the same effect as the RESET button on the front panel of the switch. It will take approximately thirty (30) seconds to complete the system boot.

Parameter description:

Save and Reboot:

Saves the current settings as the start configuration before rebooting the switch.

Reboot:

Reboots the system directly.

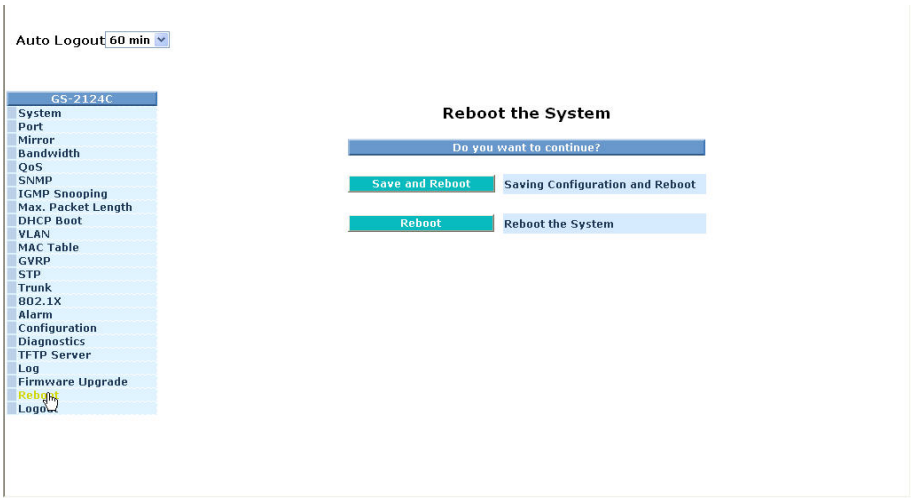


Fig. 3-70

3-23. Logout

The user can manually logout of the switch management software by performing the Logout function. The switch also provides an automatic logout capability, which is user-configured.

Function name:

Logout

Function description:

The switch allows the user to log out of the system to prevent other users from using the system without permission. If the user does not logout and exits the browser, the switch will automatically log the user out. Besides this manual logout and implicit logout, the user can pull down the **<Auto Logout>** list at the left-top corner to explicitly turn this logout function ON or OFF.

Parameter description:

Auto Logout:

Default is ON. If it is “ON”, and no action is taken and no keystroke has occurred as well in any function screen for more than 3 minutes, the switch will log the user out automatically.

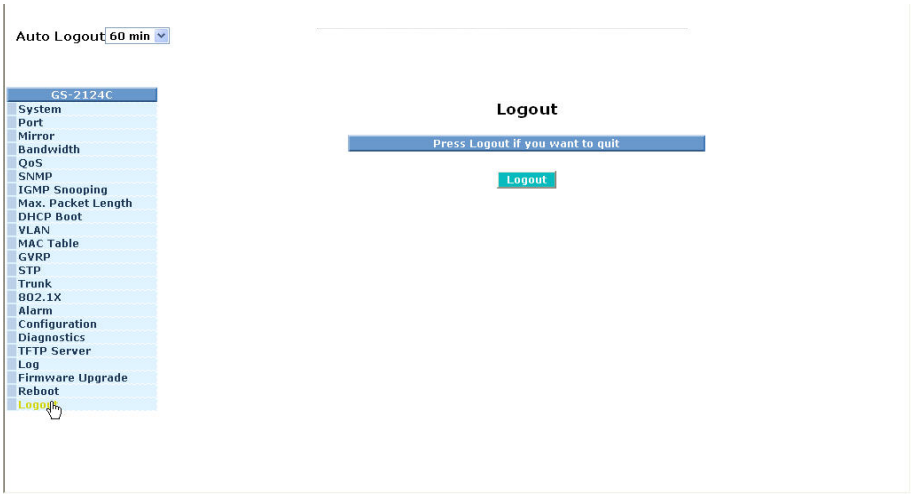


Fig. 3-71

4. Operation of CLI Management

4-1. CLI Management

Please refer to Chapter 2 for basic switch installation procedures. The following is a brief description of the procedure used to make the network connection.

-- Locate the correct DB-9 null modem cable with two female DB-9 connectors. A null modem cable is packaged with the managed switch. Please refer to Appendix B for the null modem cable configuration.

-- Attach the DB-9 female connector to the male DB-9 serial port connector on the managed switch.

-- Attach the other end of the DB-9 cable to an ASCII terminal emulator or the PC's Com1 or Com2 port. For example, a PC running Microsoft Windows' HyperTerminal utility.

-- At the "Com Port Properties" Menu, configure the parameters as below:

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4-1-1. Login

The command-line interface (CLI) is a text-based interface. The user can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin
Password: admin

After logging in successfully, the prompt will be shown as "#" if you are the first person logged in and your authorization is administrator; otherwise it will show "**$**". Please see the following two figures. The former means you have been authenticated as an administrator and have full access rights on the system. The latter means you have guest access rights and are only allowed to view the system, without permission to apply any settings to this switch.

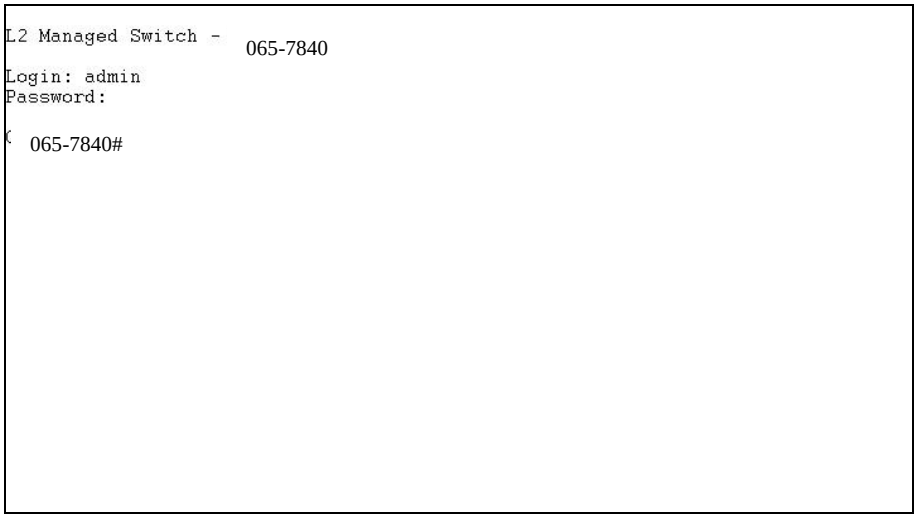

L2 Managed Switch - 065-7840
Login: admin
Password:
065-7840#

Fig. 4-1

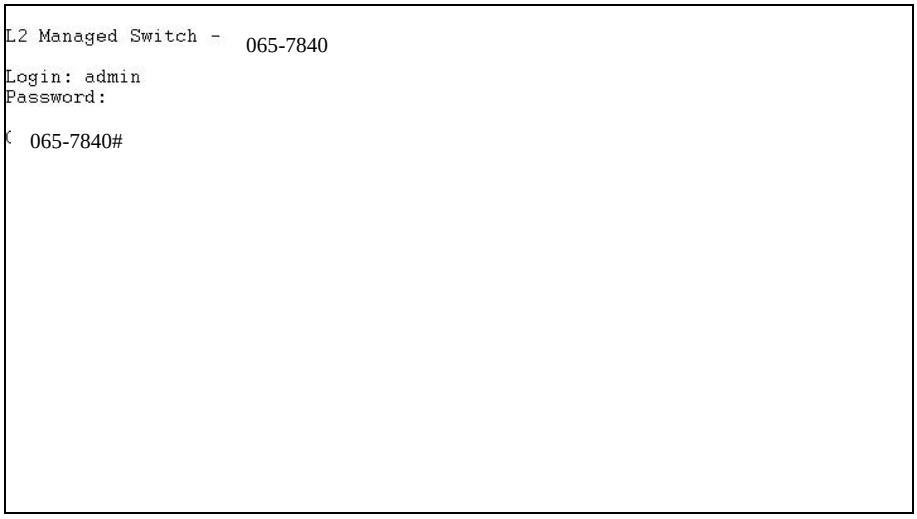

L2 Managed Switch - 065-7840
Login: admin
Password:
065-7840#

Fig. 4-2

4-2. CLI Commands

To see the commands of the CLI mode, please input "**?**" after the prompt, and then all available commands will be listed in the screen. All commands can be divided into two categories: global commands and local commands. Global commands can be used in any mode. They are "exit", "end", "help", "history", "logout", "save start", "save user", "restore default" and "restore user". For more details, please refer to Section 4-2-1.

Command instructions residing in the corresponding modes are local commands. The same command with the same command name may occur but perform totally different functions in different modes. For example, "show" in the IP mode displays the IP information; however, it displays the system information when the user is in the system mode. For more details, please refer to Section 4-2-2.

```
L2 Managed Switch -  065-7840

Login: admin
Password:

065-7840# ?
  system              Enter into system mode
  ip                  Enter into ip mode
  time                Enter into time mode
  account             Enter into account mode
  port                Enter into port mode
  mirror              Enter into mirror mode
  bandwidth           Enter into bandwidth mode
  qos                 Enter into qos mode
  snmp                Enter into snmp mode
  max-pkt-len         Enter into max packet length mode
  igmp                Enter into igmp mode
  dhcp-boot           Enter into dhcp-boot mode
  vlan                Enter into vlan mode
  mac-table           Enter into mac table mode
  gvrp                Enter into gvrp mode
  stp                 Enter into stp mode
  trunk               Enter into trunk mode
  802.1x              Enter into 802.1x mode
```

Fig. 4-3

4-2-1. CLI Global Commands

exit

Syntax:
exit
Description:
Back to the previous mode.
When the user enters this command, the user's current position would move back to the previous mode. If this command is used in the top mode, the user remains in the top mode.
Argument:
None.
Possible value:
None.
Example:

```
065-7840# trunk
065-7840(trunk)# exit

065-7840#
```

end

Syntax:
end
Description:
Back to the top mode.
When the user enters this command, the user's current position would move to the top mode. If this command is used in the top mode, the user remains in the top mode.
Argument:
None.
Possible value:
None.
Example:

```
065-7840# alarm
065-7840(alarm)# events
065-7840(alarm-events)# end

065-7840#
```

help

Syntax:
help
Description:
Shows the available commands.
Some commands are a combination of more than two words. When this command is entered, the CLI would show the complete list of commands. This command also helps the user to classify the commands between local and global commands.
Argument:
None.
Possible value:
None.
Example:

```
065-7840# ip
065-7840(ip)# help
Commands available:
  ------------<< Local commands >>------------
  set ip               Set ip,subnet mask and gateway
  set dns              Set dns
  enable dhcp          Enable DHCP, and set dns auto or manual
  disable dhcp         Disable DHCP
  show                 Show IP Configuration
  ------------<< Global commands >>------------
  exit                 Back to the previous mode
  end                  Back to the top mode
  help                 Show available commands
  history              Show a list of previously run commands
  logout               Log out of the system
  save start           Save as start config
  save user            Save as user config
  restore default      Restore default config
  restore user         Restore user config

065-7840(ip)#
```

history

Syntax:
history [#]
Description:
Shows a list of commands the user had previously run.
When this command is entered, the CLI will show a list of commands which the user had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list the total records up to 256. If an optional argument is given, the CLI would only show the last number of records stated in the argument.
Argument:
[#]: show last number of history records. (optional)
Possible value:
[#]: 1, 2, 3, …., 256
Example:

```
065-7840(ip)# history
 Command history:
  0. trunk
  1. exit
  2. 065-7840# trunk
  3. 065-7840(trunk)# exit
  4. 065-7840#
  5. ?
  6. trunk
  7. exit
  8. alarm
  9. events
 10. end
 11. ip
 12. help
 13. ip
 14. history

065-7840(ip)# history 3
 Command history:
 13. ip
 14. history
 15. history 3

065-7840(ip)#
```

logout

Syntax:
logout
Description:
When this command is entered via a Telnet connection, the user would log out of the system and disconnect. If connected to the system through the direct serial port connection with an RS-232 cable, the user would log out of the system and be back to the initial login prompt when this command is entered.
Argument:
None.
Possible value:
None.
Example:
None.

save start

Syntax:
save start
Description:
Saves the current configuration as the start configuration. When this command is entered, the CLI would save the current configuration into the non-volatile FLASH memory. If it is desired that the configuration still work after rebooting, save the configuration using the command ‘save start’.
Argument:
None.
Possible value:
None.
Example:
065-7840# save start
Saving start...
Save Successfully

065-7840#

save user

Syntax:
save user
Description:
Saves the current configuration as the user-defined configuration. When this command is entered, the CLI would save the current configuration into the non-volatile FLASH memory as a user-defined configuration.
Argument:
None.
Possible value:
None.
Example:
065-7840# save user
Saving user...
Save Successfully

065-7840#

restore default

Syntax:
restore default
Description:
Restores the factory default configuration as the startup configuration. If the default configuration restores successfully, the CLI will prompt the user to ask if an immediate reboot is desired. If the user presses Y or y, the system will reboot immediately; other responses will send the user back to the CLI system. After restoring the default configuration, all the changes in the startup configuration will be lost. After rebooting, the entire startup configuration will reset to factory default.
Argument:
None.
Possible value:
None.
Example:
065-7840# restore default
Restoring ...
Restore Default Configuration Successfully
Press any key to reboot system.

restore user

Syntax:
restore user
Description:
Restores the startup configuration as the user-defined configuration. If the default configuration restores successfully, the CLI will prompt the user to ask if an immediate reboot is desired. If the user presses Y or y, the system will reboot immediately; other responses will send the user back to the CLI system. After restoring the user-defined configuration, all the changes in the startup configuration will be lost. After rebooting, the entire startup configuration will reset to the user-defined configuration.
Argument:
None
Possible value:
None
Example:
065-7840# restore user
Restoring ...
Restore User Configuration Successfully
Press any key to reboot system.

4-2-2. CLI Local Commands

■ system

show

Syntax:
show
Description:
Displays the basic information of the switch.
Argument:
None
Possible value:
None
Example:

```
065-7840(system)# show
Model Name                    : 065-7840
System Description            : L2 Managed Switch
Location                      :
Contact                       :
Device Name                   : 065-7840
System Up Time                : 0 Days 1 Hours 19 Mins 17 Secs
Current Time                  : Fri Nov 13 01:26:11 2004
BIOS Version                  : v1.00
Firmware Version              : v0.95
Hardware-Mechanical Version   : v1.00-v1.00
Series Number                 : 123456789012
Host IP Address               : 192.168.1.1
Host MAC Address              : 00-40-c7-e7-00-04
Device Port                   : UART * 1, TP * 22, Dual-Media Port(RJ45/SFP)
* 2
RAM Size                      : 16 M
Flash Size                    : 2 M
```

set location

Syntax:
set location <location string>
Description:
Sets the location description of the switch.
Argument:
String length up to 32 characters.
Possible value:
A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:

```
065-7840(system)# set location Miami
```

set contact

Syntax:
set contact <contact string>
Description:
Sets the contact description of the switch.
Argument:
String length up to 32 characters.
Possible value:
A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
065-7840(system)# set contact 8004462377

set device-name

Syntax:
set device-name <string>
Description:
Sets the device name description of the switch.
Argument:
String length up to 32 characters.
Possible value:
A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
065-7840(system)# set device-name 065-7840

■ IP

set ip

Syntax:
set ip <ip> <mask> <gateway>
Description:
Sets the system IP address, subnet mask and gateway.
Argument:
<ip> : ip address
<mask> : Subnet Mask
<gateway> : Default Gateway
Possible value:
<ip> : 192.168.1.2 or others
<mask> : 255.255.255.0 or others
<gateway> : 192.168.1.253 or others
Example:
065-7840(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
set system IP address : 192.168.1.2
subnet mask : 255.255.255.0
default gateway : 192.168.1.253

set dns

Syntax:
set dns <ip address>
Description:
Sets the IP address of the DNS server.
Argument:
<ip address> : dns ip address
Possible value:
168.95.1.1
Example:
065-7840 (ip)# set dns 168.95.1.1
set DNS server IP address to 168.95.1.1

enable dhcp

Syntax:
enable dhcp <manual|auto>
Description:
Enables the system DHCP function and sets the DNS server via manual or auto mode.
Argument:
<manual|auto> : set dhcp by using manual or auto mode.
Possible value:
Manual or auto
Example:
065-7840(ip)# enable dhcp manual
: Enabled system DHCP function and set DNS server via manual mode.

disable dhcp

Syntax:
disable dhcp
Description:
Disables the DHCP function of the system.
Argument:
None
Possible value:
None
Example:
065-7840(ip)# disable dhcp
: Disabled system DHCP function.

show

Syntax:
show
Description:
Displays the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.
Argument:
None
Possible value:
None
Example:
065-7840(ip)# show

```
DHCP            : Disable
IP Address      : 192.168.2.65
Subnet mask     : 255.255.255.0
Gateway         : 192.168.2.252
DNS Setting     : Manual
DNS Server      : 168.95.1.1
Current IP      : 192.168.2.65
```

■ time

set manual

Syntax:
set manual <YYYY/MM/DD> <hh:mm:ss>
Description:
Sets up the current time, manually.
Argument:
<YYYY/MM/DD> <hh:mm:ss>
Possible value:
YYYY : Year (2000-2036)
MM : Month (01-12)
DD : Day (01-31)
hh : Hour (00-23)
mm : Minute (00-59)
ss : Second (00-59)
Example:
065-7840(time)# set manual 2004/12/23 16:18:00
065-7840(time)#

set ntp

Syntax:
set ntp <ip> <timezone>
Description:
Sets up the current time via the NTP server.
Argument:
ip : ntp server ip address or domain name
timezone : time zone (GMT), range: -12 to +13
Possible value:
Timezone: -12,-11…,0,1…,13
Example:
065-7840(time)# set ntp 210.59.157.10 8
065-7840(time)#

set daylightsaving

Syntax:
set daylightsaving <hr> <s:MM/DD/hh> <e:MM/DD/hh>
Description:
Sets up daylight savings time offset, start date and time, and end date and time.
Argument:
<hr> <s:MM/DD/hh> <e:MM/DD/hh>
Possible value:
hr : daylight saving hour, range: -5 to +5
s: : daylight saving start month/day/hour
e: : daylight saving end month/day/hour
MM : Month (01-12)
DD : Day (01-31)
hh : Hour (00-23)
Example:
065-7840(time)# set daylightsaving 3 10/12/01 11/12/01
Save Successfully

065-7840(time)#

show

Syntax:
show
Description:
Shows the time configuration, including “Current Time”, “NTP Server”,” Timezone”, ” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”
Argument:
None.
Possible value:
None.
Example:

```
065-7840(time)# show
Current Time                : Thu Thu 14 15:04:03 2005
NTP Server                  : 209.81.9.7
Timezone                    : GMT+8:00
Day light Saving            : 0 Hours
Day light Saving Start      : Mth: 1 Day: 1 Hour: 0
Day light Saving End  : Mth: 1 Day: 1 Hour: 0
065-7840(time)#
```

■ account

add

Syntax:
add guest <name>
Description:
Creates a new guest user. When a new guest user is created, the user must type in their password and confirm their password.
Argument:
<name> : new account name
Possible value:
A string must be at least 5 characters.
Example:

```
065-7840(account)# add aaaaa
Password:
Confirm Password:
Save Successfully
065-7840(account)#
```

del

Syntax:
del <name>
Description:
Deletes an existing user account.
Argument:
<name> : existing user account
Possible value:
None.
Example:

```
065-7840(account)# del aaaaa
Account aaaaa deleted
```

modify

Syntax:
modify <name>
Description:
Changes the username and password of an existing account.
Argument:
<name> : existing user account
Possible value:
None.
Example:

```
065-7840(account)# modify aaaaa
username/password: the length is from 5 to 15.
Current username (aaaaa):bbbbb
New password:
Confirm password:
Username changed successfully.
Password changed successfully.
```

show

Syntax:
show
Description:
Shows system account information, including account name and identity.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(account)# show
Account Name   Identity
---------------     --------
admin            : Manager
guest            : guest
```

■ port

set speed-duplex

Syntax:
set speed-duplex <range> <auto|10half|10full|100half|100full|1Gfull>
Description:
Sets up the speed and duplex mode of all ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<port-speed>:
auto: set auto-negotiation mode
10half: set speed/duplex 10M Half
10full: set speed/duplex 10M Full
100half: set speed/duplex 100M Half
100full: set speed/duplex 100M Full
1Gfull: set speed/duplex 1G Full.
Possible value:
<range>: 1 to 24
<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull
Example:
065-7840(port)# set speed-duplex 5 auto

show status

Syntax:
show status
Description:
Displays the port's current status.
Argument:
None
Possible value:
None
Example:
065-7840 (port)# show status

show simple-counter

Syntax:
show simple-counter
Description:
Displays the summary counts of each port's traffic.
Argument:
None
Possible value:
None
Example:
065-7840 (port)# show simple-counter

show detail-counter

Syntax:
Show detail-counter <range>
Description:
Displays the detailed count numbers of each port's traffic.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
1 ~ 24
Example:
065-7840 (port)# show detail-counter 5

show conf

Syntax:
show conf
Description:
Displays each port's configuration regarding state, speed, duplex mode, and flow control.
Argument:
None
Possible value:
None
Example:
065-7840 (port)# show conf

show sfp

Syntax:
show sfp <port>
Description:
Displays the SFP module information.
Argument:
<port>: available 23, 24
Possible value:
23, 24
Example:
065-7840 (port)# show sfp 23

clear counter

Syntax:
clear counter
Description:
Clears all ports' counter information (includes simple and detail port counters).
Argument:
None
Possible value:
None
Example:
065-7840 (port)# clear counter

enable state

Syntax:
enable state <range>
Description:
Enables the communication capability of the port.
Argument:
range syntax: 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
065-7840 (port)# enable state 3-12

enable flow-control

Syntax:
enable flow-control <range>
Description:
Enables the flow control function of the port.
Argument:
range syntax: 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
065-7840 (port)# enable flow-control 3-8

disable state

Syntax:
disable state <range>
Description:
Disables the communication capability of the port.
Argument:
range syntax: 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
065-7840 (port)# disable state 12

disable flow-control

Syntax:
disable flow-control <range>
Description:
Disables the flow control function of the port.
Argument:
range syntax: 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
065-7840(port)# disable flow-control 6

■ mirror

set mirror-mode

Syntax:
set mirror-mode <rx|disable>
Description:
Sets up the Port Mirroring mode (rx mode or disable).
Argument:
<rx | disable>
rx: Enable the Mirror mode (Only mirror the packets that are received)
disable: End the mirroring function
Possible value:
None
Example:
065-7840(mirror)# set mirror-mode rx
065-7840(mirror)#

set monitoring-port

Syntax:
set monitoring-port <#>
Description:
Sets up the monitoring port of the Port Mirroring function. The user can observe the packets that the monitored port receives via this port.
Argument:
<#>: the monitoring port that is chosen for the mirror function. Only one port is allowed to be configured as the monitoring port.
Possible value:
None
Example:
065-7840(mirror)# set monitoring-port 2
065-7840(mirror)#

set monitored-port

Syntax:
set monitored-port <range>
Description:
Sets up the ports that will be monitored. The packets received by these ports will be copied to the monitoring port.
Argument:
<range>: the ports that are chosen for monitored port of the mirror function.
Possible value:
None
Example:
065-7840(mirror)# set monitored-port 3-5,8,10
065-7840(mirror)#

show

Syntax:
Show
Description:
Displays the status of the Port Mirroring function settings.
Argument:
None
Possible value:
None
Example:
065-7840(mirror)# show
Mirror Mode : rx
Monitoring Port : 2
Monitored Port : 3 4 5 7 10
065-7840(mirror)#

■ bandwidth

enable ingress-rate

Syntax:
enable ingress-rate <range> <data_rate>
Description:
Sets up the ingress data rate of the ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<data_rate>: 0-1000.
Possible value:
<range>: 1 to 24
<data_rate>: 0-1000.
Example:
065-7840(bandwidth)# enable ingress-rate 1-16 100

enable storm-rate

Syntax:
enable storm-rate <range> <data_rate>
Description:
Sets up the storm data rate of the ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<data_rate>: 0-1000.
Possible value:
<range>: 1 to 24
<data_rate>: 0-1000.
Example:
065-7840(bandwidth)# enable strom-rate 1-16 150

enable egress-rate

Syntax:
enable egress-rate <range> <data_rate>
Description:
Sets up the egress data rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<data_rate>: 0-1000.
Possible value:
<range>: 1 to 24
<data_rate>: 0-1000.
Example:
065-7840(bandwidth)# enable egress-rate 1-16 200.

disable ingress-rate

Syntax:
disable ingress-rate <range>
Description:
Cancels the ingress data rate setting of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
065-7840(bandwidth)# disable ingress-rate 1-8

d*isable storm-rate*

Syntax:
disable ingress-rate <range>
Description:
Cancels the storm data rate setting of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
065-7840(bandwidth)# disable storm-rate 1-8

d*isable egress-rate*

Syntax:
disable egress-rate <range>
Description:
Cancels the egress data rate setting of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
065-7840(bandwidth)# disable egress-rate 1-8

show

Syntax:
show
Description:
Displays all current bandwidth control settings.
Argument:
None
Possible value:
None
Example:
065-7840(bandwidth)# show

	All State	All Rate	Storm State	Storm Rate	All state	All Rate
1	Disabled	0	Disabled	0	Disabled	0
2	Disabled	0	Disabled	0	Disabled	0
3	Disabled	0	Disabled	0	Disabled	0
4	Disabled	0	Disabled	0	Disabled	0
5	Disabled	0	Disabled	0	Disabled	0
6	Disabled	0	Disabled	0	Disabled	0
7	Disabled	0	Disabled	0	Disabled	0
8	Disabled	0	Disabled	0	Disabled	0
9	Disabled	0	Disabled	0	Disabled	0
10	Disabled	0	Disabled	0	Disabled	0
11	Disabled	0	Disabled	0	Disabled	0
12	Disabled	0	Disabled	0	Disabled	0
13	Disabled	0	Disabled	0	Disabled	0
14	Disabled	0	Disabled	0	Disabled	0
15	Disabled	0	Disabled	0	Disabled	0
16	Disabled	0	Disabled	0	Disabled	0
17	Disabled	0	Disabled	0	Disabled	0
18	Disabled	0	Disabled	0	Disabled	0
19	Disabled	0	Disabled	0	Disabled	0
20	Disabled	0	Disabled	0	Disabled	0
21	Disabled	0	Disabled	0	Disabled	0
22	Disabled	0	Disabled	0	Disabled	0
23	Disabled	0	Disabled	0	Disabled	0
24	Disabled	0	Disabled	0	Disabled	0

■ QoS

set mode

Syntax:
set mode <port/pri_tag/tos/layer4/diffserv>
Description:
Sets the QoS priority mode of the switch
Argument:
port: per port priority
pri_tag: vlan tag priority
tos: ip tos classification
layer4: ip tcp/udp port classification
diffserv: ip diffserv classification
Possible value:
port/pri_tag/tos/layer4/diffserv
Example:
065-7840(qos)# set mode port

set default

Syntax:
set default <class>
Description:
Sets the priority class of the packets that QoS won't affect.
Argument:
class: class of service
Possible value:
setting. 1: high, 0: low
Example:
065-7840(qos)# set default 1

set port

Syntax:
set port <range> <class>
Description:
Sets the class of ports on port-based QoS.
Argument:
<range> : port range
<class> : class of service setting.
Possible value:
<range>: syntax: 1,5-7, available from 1 to 24
<class>: 1: high, 0: low
Example:
065-7840(qos)# set port 1-10 1

set pri-tag

Syntax:
set pri_tag <port-range> <tag-range> <class>
Description:
Sets the class of ports on VLAN tag-based QoS.
Argument:
<port-range>: port range
<tag-range>: tag priority level
<class>: class of service
Possible value:
<port-range>: syntax: 1,5-7, available from 1 to 24
<tag-range>: priority level, syntax: 1,5-7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low
Example:
```
065-7840(qos)# set pri-tag 1-15 1-2 1
```

set tos

Syntax:
set tos <port-range> <tos-range> <class>
Description:
Sets the class of ports on IP ToS QoS.
Argument:
<port-range>: port range
<tos-range>: tos precedence field
<class>: class of service
Possible value:
<port-range>: syntax: 1,5-7, available from 1 to 24
<tos-range>: syntax: 1,5-7, available from 0 to 7
<class>: 1: high, 0: low
Example:
```
065-7840(qos)# set tos 1-5 0-3 0
```

set simple-layer4

Syntax:
set simple-layer4 <#>
Description:
Sets the class of ports in the simple mode of Layer 4 QoS.
Argument:
<#:> layer-4 configuration mode

Possible value:
<#:> valid values are following:
0: disable ip tcp/udp port classification
1: down prioritize web browsing, e-mail, FTP and news
2: prioritize ip telephony (VoIP)
3: prioritize iSCSI
4: prioritize web browsing, e-mail, FTP transfers and news
5: prioritize streaming Audio/Video
6: prioritize databases (Oracle, IBM DB2, SQL, Microsoft)
Example:
065-7840(qos)# set simple-layer4 2

set advance-layer4

Syntax:
set advance-layer4 <port-range> <#> <tcp/udp port> <default> <match>
Description:
Sets the class of ports in the advanced mode of Layer 4 QoS.
Argument:
<port-range>: port range
<#:> tcp/udp port number, range: 1-10
tcp/udp port range: 0-65535.
match: special TCP/UDP class. 1: high, 0: low
default: default class (all other TCP/UDP ports). 1: high, 0: low
Possible value:
Valid values are following:
<port-range>: syntax: 1,5-7, available from 1 to 24
<#:> tcp/udp port number, range: 1-10
<tcp/udp port range>: 0-65535.
match: special TCP/UDP class. 1: high, 0: low
default: default class (all other TCP/UDP ports). 1: high, 0: low
Example:
065-7840(qos)# set advance-layer4 5 2 80 1 0

set diffserv

Syntax:
set diffserv <ds-range> <class>
Description:
Sets the class of ports on IP DiffServ QoS.
Argument:
<ds-range>: dscp field
<class>: class of service
Possible value:
<ds-range>: syntax: 1,5-7, available from 0 to 63
<class>: 1: high, 0: low
Example:
065-7840(qos)# set diffserv 0-20 1

show

Syntax:
show
Description:
Displays the information of the mode chosen.
Argument:
None
Possible value:
None
Example:
065-7840 (qos)# show
IP Diffserv Classification

Default Class:high

DiffServ	Class	DiffServ	Class	DiffServ	Class	DiffServ	Class
0	high	1	high	2	high	3	high
4	high	5	high	6	high	7	high
8	high	9	high	10	high	11	high
12	high	13	high	14	high	15	high
16	high	17	high	18	high	19	high
20	high	21	high	22	high	23	high
24	high	25	high	26	high	27	high
28	high	29	high	30	high	31	high
32	high	33	high	34	high	35	high
36	high	37	high	38	high	39	high
40	high	41	high	42	high	43	high
44	high	45	high	46	high	47	high
48	high	49	high	50	high	51	high
52	high	53	high	54	high	55	high
56	high	57	high	58	high	59	high
60	high	61	high	62	high	63	high

■ snmp

enable

Syntax:
enable snmp
enable set-ability
Description:
Enables the activation of SNMP or set-community.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(snmp)# enable snmp
065-7840(snmp)# enable set-ability
```

disable

Syntax:
disable snmp
disable set-ability
Description:
Disables (deactivates) SNMP or set-community.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(snmp)# disable snmp
065-7840(snmp)# disable set-ability
```

set

Syntax:
set get-community <community>
set set-community <community>
set trap <#> <ip> [port] [community]
Description:
Set is used for the setup of get-community, set-community, trap host ip, host port and trap- community.
Argument:
<#>: trap number
<ip>: ip address or domain name
<port>: trap port
<community>:trap community name
Possible value:
trap number: 1 to 6
port:1~65535
Example:

```
065-7840(snmp)# set get-community public
065-7840(snmp)# set set-community private
065-7840(snmp)# set trap 1 192.168.1.1 162 public
```

show

Syntax:
show
Description:
Displays the SNMP configuration.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(snmp)# show
SNMP         : Enable
Get Community: public
Set Community: private [Enable]
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public
```

■ max-pkt-len

set len

Syntax:
set len <range> <length>
Description:
Sets the maximum packet length for a port or a range of ports.
Argument:
<range> Port range
<length >(bytes): Maximum Packet Length can be accepted
Possible value:
<range> : syntax 1,5-7, available from 1 to 24
<length>(bytes): 1518/1532/9216
Example:
065-7840(max-pkt-len)# set len 1-8 9216

show

Syntax:
show
Description:
Shows the current Maximum Packet Length setting for all ports on the switch.
Argument:
None
Possible value:
None
Example:
065-7840(max-pkt-len)# show

PORT	Max Packet Length
1	1518
2	1518
3	1518
4	1518
5	1518
6	1518
7	1518
8	1518
9	1518
10	1518
11	1518
12	1518
13	1518
14	1518
15	1518
16	1518
17	1518
18	1518
19	1518
20	1518
21	1518
22	1518
23	1518
24	1518

■ igmp

set igmp_snooping

Syntax:
set igmp_snooping <status>
Description:
Sets up the IGMP Snooping mode.
Argument:
<status> 0:disable , 1:active , 2:passive
Possible value:
<status> 0,1,2
Example:
065-7840(igmp)# set igmp-snooping 2

show

Syntax:
show
Description:
Displays the IGMP snooping mode status and the IP Multicast Table.
Argument:
None
Possible value:
None
Example:
065-7840(igmp)# show
Snoop Mode: Active

IP Multicast:
1) IP Address : 224.1.1.1
VLAN ID : 0
Member Port : 22

■ dhcp-boot

set dhcp-boot

Syntax:
set dhcp-boot <sec>
Description:
Sets up the delay time for DHCP Boot.
Argument:
<sec>:range syntax: 0, 1-30. The value “0” is to disable dhcp-boot delay
Possible value:
<sec>:0-30
Example:
065-7840(dhcp-boot)# set dhcp-boot 30

show

Syntax:
show
Description:
Displays the DHCP Boot status.
Argument:
None
Possible value:
None
Example:
065-7840(DHCP-BOOT)# SHOW
DHCP BOOT : ENABLE
Second : 10

■ VLAN

set mode

Syntax:
set mode <disable|port|tag|metro|double-tag> [uplink]
Description:
Sets the switch's VLAN mode for a port or a range of ports, including disable, port-based, tag-based, metro and double-tag modes.
Argument:
disable: VLAN disable
tag: set tag-based VLAN
port: set port-based VLAN
metro: set metro mode VLAN
double-tag: enable Q-in-Q function
uplink syntax: 1,5-7, available from 23 to 24, only for metro mode VLAN
Possible value:
<disable|port|tag|metro|double-tag>: disable,port,tag,metro,double-tag
[uplink]: 23 or 24 or "23,24"
Example:
065-7840(vlan)# set mode metro 23-24

set tag-group

Syntax:
set tag-group <vid> <name> <range> <#>
Description:
Adds or edits the tag-based VLAN group.
Argument:
vid: VLAN ID
name: VLAN name
range: VLAN group members, syntax: 1,5-7
#: sym/asym VLAN setting. 1: symmetric VLAN, 0: asymmetric VLAN
Possible value:
vid: range from 1 to 4094
name: tag- VLAN name
range: from 1 to 24
:0,1
Example:
065-7840(vlan)# set tag-group 2 VLAN-2 2-5,6,15-13 0

set port-group

Syntax:
set port-group <name> <range>
Description:
Adds or edits a port-based VLAN group.
Argument:
name: VLAN name
range: VLAN group members, syntax: 1,5-7
Possible value:
name: port- VLAN name
range: available from 1 to 24
Example:
065-7840(vlan)# set port-group vlan-1 2-5,6,15-13

set mode metro [uplink]

Syntax:
set mode metro [uplink]
Description:
Creates metro groups, and select a port(s) as the uplink port(s).
Argument:
Uplink: You can choose port 23 as “23”, port 24 as “24”, or port 23&24 as “23,24”,”23-24”.If you do not choose any uplink port, system will take port 24.
Possible value:
[uplink]: 23 or 24 or “23,24” or “23-24”
Example:
065-7840(vlan)# set mode metro 23-24

set pvid

Syntax:
set pvid <range> <pvid>
Description:
Sets the PVID of a VLAN.
Argument:
Range: which port(s) you want to set PVID(s).
syntax: 1,5-7
pvid: which PVID(s) you want to set.
Possible value:
Range: available from 1 to 24
pvid: available from 1 to 4094
Example:
065-7840(vlan)# set pvid 3,5,6-8 5

set port-role

Syntax:
set port-role <range> <access|trunk|hybrid> [vid]
Description:
Sets egress rule: configures the port roles.
Argument:
range :which port(s) you want to set.
access: Do not tag frames
trunk: Tag all frames
hybrid: Tag all frames except a specific VID
vid: untag-vid for hybrid port
Possible value:
range : available from 1 to 24
vid: available from 1 to 4094
Example:
065-7840(vlan)# set port-role 5 hybrid 6

enable sym-vlan <range>

Syntax:
enable sym-vlan <range>
Description:
Enables dropping frames from the non-member port.
Argument:
range : which port(s) you want to set. Syntax: 1,5-7
Possible value:
range: available from 1 to 24
Example:
065-7840(vlan)# enable sym-vlan 5-10

disable sym-vlan

Syntax:
disable sym-vlan <range>
Description:
Disables dropping frames from the non-member port.
Argument:
range : which port(s) you want to set.
Possible value:
range: available from 1 to 24
Example:
065-7840(vlan)# disable sym-vlan 5-10

enable drop-untag

Syntax:
enable drop-untag <range>
Description:
Enables dropping the untagged frames.
Argument:
range: which port(s) you want to set.
Possible value:
range: available from 1 to 24
Example:
065-7840(vlan)# enable drop-untag 5-10

disable drop-untag

Syntax:
disable drop-untag <range>
Description:
Disables dropping of the untagged frames.
Argument:
range : which port(s) you want to set. Syntax: 1,5-7
Possible value:
range: available from 1 to 24
Example:
065-7840(vlan)# disable drop-untag 5-10

del tag-group <vid>

Syntax:
del tag-group <vid>
Description:
Deletes a tag-based VLAN group.
Argument:
vid: which VLAN group you want to delete.
Possible value:
vid: available from 1 to 4094
Example:
065-7840(vlan)# del tag-group 2

del port-group <name>

Syntax:
del port-group <name>
Description:
Deletes a port-based VLAN group.
Argument:
name: which VLAN group you want to delete.
Possible value:
name: port- VLAN name
Example:
065-7840(vlan)# del port-group VLAN-2

show group

Syntax:
show group
Description:
Displays the VLAN mode and VLAN group.
Argument:
None
Possible value:
None
Example:

```
065-7840(vlan)# show group
Vlan mode is double-tag.

1)  Vlan Name : default
    Vlan ID   : 1
    Sym-vlan  : Disable
    Member    : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

2)  Vlan Name : VLAN-2
    Vlan ID   : 2
    Sym-vlan  : Disable
    Member    : 2 3 4 5 6 13 14 15
 065-7840(vlan)#
```

show pvid

Syntax:
show pvid
Description:
Displays PVID, displays ingress/egress rules.
Argument:
None
Possible value:
None
Example:

```
065-7840(vlan)# show pvid
 Port   PVID    Rule1     Rule2    Port Rule   Untag Vid
------ ------ --------- --------- ----------- -----------
   1       1   Disable   Disable     Access         -
   2       1   Disable   Disable     Access         -
   3       5   Disable   Disable     Access         -
   4       1   Disable   Disable     Access         -
   5       5   Enable    Disable     Hybrid         6
   6       5   Enable    Disable     Access         -
   7       5   Enable    Disable     Access         -
   8       5   Enable    Disable     Access         -
   9       1   Enable    Disable     Access         -
  10       1   Enable    Disable     Access         -
  11       1   Disable   Disable     Access         -
  12       1   Disable   Disable     Access         -
  13       1   Disable   Disable     Access         -
  14       1   Disable   Disable     Access         -
  15       1   Disable   Disable     Access         -
  16       1   Disable   Disable     Access         -
  17       1   Disable   Disable     Access         -
  18       1   Disable   Disable     Access         -
  19       1   Disable   Disable     Access         -
  20       1   Disable   Disable     Access         -
  21       1   Disable   Disable     Access         -
  22       1   Disable   Disable     Access         -
...(q to quit)

  23       1   Disable   Disable     Access         -
  24       1   Disable   Disable     Access         -

065-7840(vlan)#
```

■ mac-table

<<information>>

show

Syntax:
Show
Description:
Displays all MAC table information.
Argument:
None
Possible value:
None
Example:
065-7840(mac-table-information)# show
MAC Table List
Alias MAC Address Port VID State
---------- ---------- ---- ---- ----------

065-7840(mac-table-information)#

search

Syntax:
search <port> <mac> <vid>
Description:
Looks for the relative MAC information in the MAC table.
Argument:
<port> : set up the range of the ports to search for,
syntax: 1,5-7, available form 1 to 24
<mac> : MAC address, format: 01-02-03-04-05-06, '?' can be used
<vid> : vid: vlan id, from 1 to 4094; '?' as don't care, 0 as untagged
Possible value:
None
Example:

```
065-7840(mac-table-information)# search 1-24 ??-??-??-??-??-?? ?
MAC Table List
Alias            MAC Address       Port VID  State
---------------- ----------------- ---- ---- -----------------
                 00-40-c7-88-00-06    1   0  Dynamic
065-7840(mac-table-information)#
```

<<maintain>>

set aging

Syntax:
set aging <#>
Description:
Sets up the age out time of a dynamic learning MAC table.
Argument:
<#> : age-timer in seconds, 0, 10 to 65535. The value zero disables aging
Possible value:
None
Example:
065-7840(mac-table-maintain)# set aging 300
065-7840(mac-table-maintain)#

set flush

Syntax:
set flush
Description:
Deletes all of the MACs that are learned dynamically.
Argument:
None
Possible value:
None
Example:
065-7840(mac-table-maintain)# set flush
065-7840(mac-table-maintain)#

show

Syntax:
show
Description:
Displays the settings of the age-timer.
Argument:
None
Possible value:
None
Example:
065-7840(mac-table-maintain)# show
age-timer : 300 seconds
065-7840(mac-table-maintain)#

<<static-mac>>

add

Syntax:
add <mac> <port> <vid> [alias]
Description:
Adds the static MAC entry.
Argument:
<mac> : MAC address, format: 00-02-03-04-05-06
<port> : 0-24. the value zero means this entry is the filtering entry
<vid> : vlan id. 0, 1-4094. vid must be zero if VLAN mode is not tag-based
[alias] : MAC alias name, max 15 characters
Possible value:
None
Example:
065-7840(mac-table-static-mac)# add 00-02-03-04-05-06 3 0 aaa
065-7840(mac-table-static-mac)#

del

Syntax:
del <mac> <vid>
Description:
Removes the static MAC entry.
Argument:
<mac> : MAC address, format: 00-02-03-04-05-06
<vid> : vlan id. 0, 1-4094. vid must be zero if VLAN mode is not tag-based
Possible value:
None
Example:
065-7840(mac-table-static-mac)# del 00-02-03-04-05-06 0
065-7840(mac-table-static-mac)#

show forward

Syntax:
show forward
Description:
Display the static forwarding table.
Argument:
None
Possible value:
None
Example:
065-7840(mac-table-static-mac)# show forward
Static Forwarding Entry: (Total 1 item(s))
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa
065-7840(mac-table-static-mac)#

show filter

Syntax:
show filter
Description:
Displays the static filtering table.
Argument:
None
Possible value:
None
Example:
065-7840(mac-table-static-mac)# show filter
Static Filtering Entry: (Total 1 item(s))
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc
065-7840(mac-table-static-mac)#

<<alias>>

set

Syntax:
set <mac> <alias>
Description:
Sets up the MAC alias entry.
Argument:
<mac> : MAC address, format: 00-02-03-04-05-06
<alias> : MAC alias name, max 15 characters
Possible value:
None
Example:
065-7840(mac-table-alias)# set 00-44-33-44-55-44 www
065-7840(mac-table-alias)#

del

Syntax:
del <mac>
Description:
Deletes the MAC alias entry.
Argument:
<mac> : MAC address, format: 00-02-03-04-05-06
Possible value:
None
Example:
065-7840(mac-table-alias)# del 00-44-33-44-55-44
065-7840(mac-table-alias)#

show

Syntax:
show
Description:
To display the MAC alias entry.
Argument:
None
Possible value:
None
Example:

```
065-7840(mac-table-alias)# show
MAC Alias List
     MAC Address       Alias
----- ----------------- ----------------
1)    00-02-03-04-05-06 aaa
2)    00-33-03-04-05-06 ccc
3)    00-44-33-44-55-66 rrr

065-7840(mac-table-alias)#
```

■ gvrp

enable

Syntax:
enable
Description:
Enables the GVRP function.
Argument:
None
Possible value:
None
Example:
065-7840(gvrp)# enable

disable

Syntax:
disable
Description:
Disables the GVRP function.
Argument:
None
Possible value:
None
Example:
065-7840(gvrp)# disable

set timer

Syntax:
set timer <range> <join> <leave> <leaveall>
Description:
Sets GVRP join time, leave time, and leaveall time for each port.
Argument:
<range> : port range
<join>: join timer
<leave>: leave timer
<leaveall>: leaveall timer

Possible value:
<range> : syntax 1,5-7, available from 1 to 24
<join>: available from 20 to 100
<leave>: available from 60 to 300
<leaveall>: available from 1000 to 5000
Leave Time must equal double Join Time at least.
Example:
065-7840(gvrp)# set timer 2-8 25 80 2000

set applicant

Syntax:
set applicant <range> <normal|non-participant>
Description:
Sets the default applicant mode for each port.
Argument:
range: port range
normal: set applicant as normal mode
non-participant: set applicant as non-participant mode

Possible value:
<range>: syntax 1,5-7, available from 1 to 24
<normal|non-participant>: normal or non-participant
Example:
065-7840(gvrp)# set applicant 1-10 non-participant

set registrar

Syntax:
set registrar <range> <normal|fixed|forbidden>
Description:
Sets the default registrar mode for each port.
Argument:
range: port range
normal: set registrar as normal mode
fixed: set registrar as fixed mode
forbidden: set registrar as forbidden mode
Possible value:
<range>: syntax 1,5-7, available from 1 to 24
<normal|fixed|forbidden>: normal or fixed or forbidden
Example:
065-7840(gvrp)# set registrar 1-5 fixed

show counter

Syntax:
show counter
Description:
Displays the GVRP counter values for Total GVRP packets and Invalid GVRP packets, along with JoinEmpty, JoinIn, LeaveAll, and LeaveEmpty, and Empty messages, for each port.
Argument:
<port>: port number
Possible value:
<port>: available from 1 to 24

Example:

```
065-7840(gvrp)# show counter 2
GVRP Counter port: 2
Counter Name           Received Transmitted
--------------------   -------- -----------
Total GVRP Packets            0           0
Invalid GVRP Packets          0        ----
LeaveAll message              0           0
JoinEmpty message             0           0
JoinIn message                0           0
LeaveEmpty message            0           0
Empty message                 0           0
```

show config

Syntax:
show config
Description:
Displays the GVRP configuration.
Argument:
none
Possible value:
none

Example:

```
065-7840(gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time    Applicant    Registrar Restricted
---- --------- ---------- ------------- ---------------- --------- ----------
  1      20         60          1000      Normal          Normal      Disable
  2      25         80          2000      Normal          Normal      Disable
  3      25         80          2000      Normal          Normal      Disable
  4      25         80          2000      Normal          Normal      Disable
  5      25         80          2000      Normal          Normal      Disable
  6      25         80          2000      Normal          Normal      Disable
  7      25         80          2000      Normal          Normal      Disable
  8      25         80          2000      Normal          Normal      Disable
  9      20         60          1000      Normal          Normal      Disable
 10      20         60          1000      Normal          Normal      Disable
 11      20         60          1000      Normal          Normal      Disable
 12      20         60          1000      Normal          Normal      Disable
 13      20         60          1000      Normal          Normal      Disable
 14      20         60          1000      Normal          Normal      Disable
 15      20         60          1000      Normal          Normal      Disable
 16      20         60          1000      Normal          Normal      Disable
 17      20         60          1000      Normal          Normal      Disable
 18      20         60          1000      Normal          Normal      Disable
 19      20         60          1000      Normal          Normal      Disable
 20      20         60          1000      Normal          Normal      Disable
 21      20         60          1000      Normal          Normal      Disable

...(q to quit)

 22      20         60          1000      Normal          Normal      Disable
 23      20         60          1000      Normal          Normal      Disable
 24      20         60          1000      Normal          Normal      Disable
```

show group

Syntax:
show group
Description:
Shows the GVRP group.
Argument:
none
Possible value:
none
Example:

```
065-7840(gvrp)# show group
GVRP group information
VID  Member Port
---- ------------------------------------------------
```

■ stp

enable

Syntax:
enable
Description:
Enables the Spanning Tree Protocol (STP) function.
Argument:
None
Possible value:
None
Example:
065-7840(stp)# enable

disable

Syntax:
disable
Description:
Disables the STP function.
Argument:
None
Possible value:
None
Example:
065-7840(stp)# disable

set config

Syntax:
set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>
Description:
Sets up the parameters of STP.
Argument:
<Bridge Priority> :Priority must be a multiple of 4096, available from 0 to 61440.
<Hello Time>: available from 1 to 10.
<Max. Age>: available from 6 to 40.
<Forward Delay>: available from 4 to 30.
Possible value:
<Bridge Priority> 0 to 61440.
<Hello Time>: 1 to 10.
<Max. Age>: 6 to 40.
<Forward Delay>: 4 to 30.
Example:
065-7840(stp)# set config 61440 2 20 15

set version

Syntax:
set version <stp|rstp>
Description:
Sets up the version of STP used by the switch [Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP)].
Argument:
<stp|rstp>:stp / rstp
Possible value:
<stp|rstp>:stp / rstp
Example:
065-7840(stp)# set version rstp

set port

Syntax:
set port <range> <path cost> <priority> <edge_port> <admin p2p>
Description:
Sets up the port information of STP.
Argument:
<range> : syntax 1,5-7, available from 1 to 24
<path cost>: 0, 1-200000000. The value zero means auto status
<priority> : priority must be a multiple of 16, available from 0 to 240
<edge_port> : Admin Edge Port, <yes|no>
<admin p2p>: Admin point to point, <auto|true|false>
Possible value:
<range> :1 to 24
<path cost>: 0, 1-200000000.
<priority> : 0 to 240
<edge_port> : yes / no
<admin p2p>: auto / true / false
Example:
065-7840(stp)# set port 1-16 0 128 yes auto

show status

Syntax:
show status
Description:
Displays the status of STP.
Argument:
None
Possible value:
None

Example:
065-7840(stp)# show status
STP Status :
STP State : Enabled
Bridge ID : 00:40:C7:D8:09:1D
Bridge Priority : 61440
Designated Root : 00:40:C7:D8:09:1D
Designated Priority : 61440
Root Port : 0
Root Path Cost : 0
Current Max. Age(sec) : 20
Current Forward Delay(sec) : 15
Hello Time(sec) : 2
STP Topology Change Count : 0
Time Since Last Topology Change(sec) : 848

show config

Syntax:
show config
Description:
Displays the configuration of STP.
Argument:
None
Possible value:
None
Example:
065-7840(stp)# show config
STP State Configuration :
Spanning Tree Protocol : Enabled
Bridge Priority (0-61440) : 61440
Hello Time (1-10 sec) : 2
Max. Age (6-40 sec) : 20
Forward Delay (4-30 sec) : 15
Force Version : RSTP

show port

Syntax:
show port
Description:
To display the port information of STP.
Argument:
None
Possible value:
None
Example:

```
065-7840# stp
065-7840(stp)# show port
Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point
==== =========== ========= ======== ================ ====================
  1  DISCARDING    2000000    128         No                Auto
  2  DISCARDING    2000000    128         No                Auto
  3  DISCARDING    2000000    128         No                Auto
  4  DISCARDING    2000000    128         No                Auto
  5  DISCARDING    2000000    128         No                Auto
  6  DISCARDING    2000000    128         No                Auto
  7  DISCARDING    2000000    128         No                Auto
  8  DISCARDING    2000000    128         No                Auto
  9  DISCARDING    2000000    128         No                Auto
 10  DISCARDING    2000000    128         No                Auto
 11  DISCARDING    2000000    128         No                Auto
 12  DISCARDING    2000000    128         No                Auto
 13  DISCARDING    2000000    128         No                Auto
 14  DISCARDING    2000000    128         No                Auto
 15  DISCARDING    2000000    128         No                Auto
 16  DISCARDING    2000000    128         No                Auto
 17  DISCARDING    2000000    128         No                Auto
 18  DISCARDING    2000000    128         No                Auto
 19  DISCARDING    2000000    128         No                Auto
 20  DISCARDING    2000000    128         No                Auto
 21  DISCARDING    2000000    128         No                Auto
 22  DISCARDING    2000000    128         No                Auto
...(q to quit)

 23  DISCARDING    2000000    128         No                Auto
 24  DISCARDING    2000000    128         No                Auto
```

■ trunk

set priority

Syntax:
set priority <range>
Description:
Sets up the LACP system priority.
Argument:
<range> : available from 1 to 65535.
Possible value:
32768
Example:
065-7840(trunk)# set priority 33333
065-7840(trunk)#

set trunk

Syntax:
set trunk <port-range> <method> <group> <active LACP>
Description:
Sets up the trunk status, including the group number and mode of the trunk as well as LACP mode.
Argument:
<port-range> : syntax 1,5-7, available from 1 to 24
<method>:
static : adopt the static link aggregation
lacp : adopt the dynamic link aggregation- link aggregation control protocol
<group>: 1-8.
<active LACP>:
active : set the LACP to active mode
passive : set the LACP to passive mode
Possible value:
None
Example:
065-7840(trunk)# set trunk 1-4 lacp 1 active
065-7840(trunk)#

del trunk

Syntax:
del trunk <port-range>
Description:
Deletes a trunk port
Argument:
<port-range> : syntax 1,5-7, available from 1 to 24
Possible value:
None
Example:
065-7840(trunk)# del trunk 1
065-7840(trunk)#

show status

Syntax:
show status
Description:
Displays the aggregator status and the settings of each port.
Argument:
None
Possible value:
None
Example:
065-7840(trunk)# show status

Trunk Port Setting				Trunk Port Status	
Port	Method	Group	Active LACP	Aggregator	Status
1	None	0	Active	1	Ready
2	LACP	1	Active	2	---
3	LACP	1	Active	3	---
4	LACP	1	Active	4	---
5	LACP	1	Active	5	---
6	LACP	1	Active	6	---
7	LACP	1	Active	7	---
8	LACP	1	Active	8	---
9	LACP	1	Active	9	---
10	LACP	1	Active	10	---
11	LACP	1	Active	11	---
12	LACP	1	Active	12	---
13	LACP	1	Active	13	---
14	LACP	1	Active	14	---
15	None	0	Active	15	---
16	None	0	Active	16	---
17	None	0	Active	17	---
18	None	0	Active	18	---
19	None	0	Active	19	---
20	None	0	Active	20	---
21	None	0	Active	21	---
22	None	0	Active	22	---
23	None	0	Active	23	---
24	None	0	Active	24	---

065-7840(trunk)#

show aggtr-view

Syntax:
show aggtr-view
Description:
Displays the aggregator list.
Argument:
None
Possible value:
None
Example:

```
065-7840(trunk)# show aggtr-view
Aggregator  1) Method: None
            Member Ports: 1
            Ready Ports:1

Aggregator  2) Method: LACP
            Member Ports: 2
            Ready Ports:
                  :
                  :
                  :
```

show lacp-detail

Syntax:
show lacp-detail <aggtr>
Description:
Displays detailed information about the LACP trunk group.
Argument:
<aggtr> : available from 1 to 24
Possible value:
None
Example:

```
065-7840(trunk)# show lacp-detail 2
Aggregator 2 Information:
              Actor                              Partner
---------------------------------- ----------------------------------
System Priority    MAC Address    System Priority    MAC Address
--------------- ----------------- --------------- -----------------
     32768       00-40-c7-e8-00-02      32768       00-00-00-00-00-00

 Port    Key       Trunk Status          Port              Key
------ -------- ------------------ --------------- -----------------
   2     257            ---               2                0

065-7840(trunk)#
```

show lacp-priority

Syntax:
show lacp-priority
Description:
Displays the LACP Priority value.
Argument:
None
Possible value:
None
Example:
065-7840(trunk)# show lacp-priority
LACP System Priority : 32768
065-7840(trunk)#

■ 802.1x

set state

Syntax:
set state <ip> <port-number> <secret-key>
Description:
Configures the settings related to the 802.1X Radius Server.
Argument:
<ip> : the IP address of Radius Server
<port-number> : the service port of Radius Server(Authorization port)
<secret-key> : set up the value of secret-key, and the length of secret-key is from 1 to 31
Possible value:
<port-number> : 1~65535, default is 1812
Example:
065-7840(802.1x)# set state 192.168.1.115 1812 WinRadius
065-7840(802.1x)#

set mode

Syntax:
set mode <port-range> <mode>
Description:
Sets up the 802.1X authentication mode of each port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<mode>: set up 802.1x mode
0:disable the 802.1x function
1:set 802.1x to Multi-host mode
Possible value:
<port range> : 1 to 24
<mode>: 0 or 1
Example:
065-7840(802.1x)# set mode 2 1
065-7840(802.1x)#

set port-control

Syntax:
set port-control <port-range> <authorized>
Description:
Sets up the 802.1X status of each port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<authorized> : Set up the status of each port
0:ForceUnauthorized
1:ForceAuthorized
2:Auto
Possible value:
<port range> : 1 to 24
<authorized> : 0, 1 or 2
Example:
065-7840(802.1x)# set port-control 2 2

set reAuthMax

Syntax:
set reAuthMax <port-range> <max>
Description:
Sets the number of reauthentication attempts that are permitted before the port becomes Unauthorized.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<max> : max. value , range 1-10
Possible value:
<port range> : 1 to 24
<max> : 1-10, default is 2
Example:
065-7840(802.1x)# set reAuthMax 2 2

set txPeriod

Syntax:
set txPeriod <port-range> <sec>
Description:
Sets the value in seconds of the timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 30
Example:
065-7840(802.1x)# set txPeriod 2 30

set quiet-period

Syntax:
set quiet-period <port-range> <sec>
Description:
Sets the value in seconds of a timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 0-65535
Possible value:
<port range> : 1 to 24
<sec> : 0-65535, default is 60
Example:
065-7840(802.1x)# set quiet-period 2 30

set reAuthEnabled

Syntax:
set reAuthEnabled <port-range> <ebl>
Description:
Sets a constant that defines whether regular reauthentication will take place on this port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<ebl> :
0:OFF Disable reauthentication
1:ON Enable reauthentication
Possible value:
<port range> : 1 to 24
<ebl> : 0 or 1, default is 1
Example:
065-7840(802.1x)# set reAuthEnabled 2 1

set reAuthPeriod

Syntax:
set reAuthPeriod <port-range> <sec>
Description:
Sets a constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 3600
Example:
065-7840(802.1x)# set reAuthPeriod 2 3600

set max-request

Syntax:
set max-request <port-range> <times>
Description:
Sets the maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<times>: max-times , range 1-10
Possible value:
<port range> : 1 to 24
<times>: 1-10, default is 2
Example:
065-7840(802.1x)# set max-request 2 2

set suppTimeout

Syntax:
set suppTimeout <port-range> <sec>
Description:
Sets a timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 30
Example:
065-7840(802.1x)# set suppTimeout 2 30
065-7840(802.1x)#

set serverTimeout

Syntax:
set serverTimeout <port-range> <sec>
Description:
Sets a timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 30
Example:
065-7840(802.1x)# set serverTimeout 2 30
065-7840(802.1x)#

show state

Syntax:
show state
Description:
Shows the Radius server configuration
Argument:
None
Possible value:
None
Example:
065-7840(802.1x)# show state
Radius Server: 192.168.1.115
Port Number : 1812
Secret Key : WinRadius

065-7840(802.1x)#

show mode

Syntax:
show mode
Description:
Displays the 802.1x mode of each port.
Argument:
None
Possible value:
None
Example:
065-7840(802.1x)# show mode

Port	Mode
1	Disable
2	Multi-host
3	Disable
4	Disable
5	Disable
6	Disable
:	
:	
:	

show security

Syntax:
show security
Description:
Displays the authentication status of each port.
Argument:
None
Possible value:
None
Example:
065-7840(802.1x)# show security

Port	Mode	Status
1	Disable	
2	Multi-host	Unauthorized
3	Disable	
4	Disable	
5	Disable	
6	Disable	
:		
:		
:		

show parameter

Syntax:
show parameter
Description:
Displays the 802.1x parameter settings of each port.
Argument:
None
Possible value:
None
Example:
065-7840(802.1x)# show parameter

```
port  1) port control  : Auto
         reAuthMax     : 2
         txPeriod      : 30
         Quiet Period  : 60
         reAuthEnabled : ON
         reAuthPeriod  : 3600
         max. Request  : 2
         suppTimeout   : 30
         serverTimeout : 30

port  2) port control  : Auto
         reAuthMax     : 2
         txPeriod      : 30
         Quiet Period  : 60
         reAuthEnabled : ON
         reAuthPeriod  : 3600
         max. Request  : 2
         suppTimeout   : 30
         serverTimeout : 30

               :
               :
               :
```

■ alarm

<<events>>

set

Syntax:
set sms <range>
set email <range>
set trap <range>
set all <range>
Description:
Activation of SMS, email and trap events.
Argument:
<range>: syntax 1,5-7, trap number.
Possible value:
available from 1 to 24.
Example:

```
065-7840(alarm-events)# set sms 1-3
065-7840(alarm-events)# set email 1-3
065-7840(alarm-events)# set trap 1-3
065-7840(alarm-events)# set all 1-3
```

del

Syntax:
del sms <range>
del email <range>
del trap <range>
del all <range>
Description:
Deactivation of SMS, email and trap events.
Argument:
<range>:trap number.
Possible value:
From 1 to 24.
Example:

```
065-7840(alarm-events)# del sms 1-3
065-7840(alarm-events)# del email 1-3
065-7840(alarm-events)# del trap 1-3
065-7840(alarm-events)# del all 1-3
```

show

Syntax:
show
Description:
Displays the configuration of alarm events.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(alarm-events)# show
   Events                    Email SMS Trap
-----------------------------------------
1  Cold Start                        v
2  Warm Start                        v
3  Link Down                         v
4  Link Up                           v
5  Authentication Failure            v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 VLAN Disabled
18 Port-based VLAN Enabled
19 Tag-based VLAN Enabled
20 Metro-mode VLAN Enabled
21 Double-tag VLAN Enabled
22 Module Inserted
23 Module Removed
24 Module Media Swapped
```

<<email>>

set

Syntax:
set server <ip>
set user <username>
set mail-address <#> <mail address>
Description:
Used to configure of e-mail server, username, password and address information.
Argument:
<ip>: E-mail server ip
<username>: email server account and password
<#>: email address number, range: 1 to 6
<mail address>: email address
Possible value:
<#>: 1 to 6
Example:

```
065-7840(alarm-email)# set server 192.168.1.6
065-7840(alarm-email)# set user admin
Password:
Confirm Password:

065-7840(alarm-email)# set mail-address 1 abc@mail.abc.com
```

del

Syntax:
del <#>
Description:
Removes the E-mail address configuration.
Argument:
<#>: email address number, range: 1 to 6
Possible value:
<#>: 1 to 6
Example:

```
065-7840(alarm-email)# del 2
```

show

Syntax:
show
Description:
Displays the configuration of an e-mail trap event.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(alarm-email)# show
Mail Server    : 192.168.1.6
Username       : admin
Password       : ***************
Email Address 1: abc@mail.abc.com
Email Address 2:
Email Address 3:
Email Address 4:
Email Address 5:
Email Address 6:
```

<<sms>>

set

Syntax:
set server <ip>
set user <username>
set phone-number <#> <phone-number>
Description:
Used to configure the SMS server, username, password and phone number.
Argument:
<ip>: SMS server ip
<username>: SMS server account and password
<#>: mobile phone number, range: 1 to 6
<phone-number>: phone number
Possible value:
<#>: 1 to 6
Example:

```
065-7840(alarm-sms)# set server 192.168.1.7
065-7840(alarm-sms)# set user ruby
Password:
Confirm Password:
065-7840(alarm-sms)# set phone-number 1 0968777777
```

del

Syntax:
del <#>
Description:
Removes the mobile phone number configuration used for reporting trap events.
Argument:
<#>: mobile phone number, range: 1 to 6
Possible value:
<#>: 1 to 6
Example:

```
065-7840(alarm-sms)# del 3
```

show

Syntax:
show
Description:
Displays the configuration of SMS trap events.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(alarm-sms)# show
SMS Server     : 192.168.1.7
Username       :
Password       : ****************
Mobile Phone  1: 0968777777
Mobile Phone  2:
Mobile Phone  3:
Mobile Phone  4:
Mobile Phone  5:
Mobile Phone  6:
```

show (alarm)

Syntax:
show
Description:
Displays Trap events, SMS alarm configuration, or E-mail alarm configuration.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(alarm)# show events
065-7840(alarm)# show email
065-7840(alarm)# show sms
```

■ diag

diag

Syntax:
diag
Description:
Used to test UART, DRAM, Flash memory, and EEPROM.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(diag)# diag
EEPROM Test : OK
UART Test   : OK
DRAM Test   : OK
Flash Test  : OK
```

Loopback

Syntax:
Loopback
Description:
Initiates an Internal/External Loopback Test.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(diag)# loopback
Internal Loopback Test : OK

External Loopback Test : Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24 Fail
```

ping

Syntax:
ping <ip>
Description:
Confirms that the remote end-station or the switch itself is alive or not.
Argument:
[ip] : ip address or domain name
Possible value:
IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com
Example:

```
065-7840(diag)# ping 192.168.1.115
Gateway      : 192.168.1.253
192.168.1.115 is alive.
```

■ log

show

Syntax:
show
Description:
Shows a list of trap log events. When any log events happen, they will be recorded and can be queried using the show command in the log function. Up to 120 log records are supported.
Argument:
None.
Possible value:
None.
Example:

```
065-7840(log)# show

TFTP Server : 0.0.0.0
Auto Upload : Disable

1)  Wed Apr 13 12:13:27 2005  Link Up [Port 1]
2)  Wed Apr 13 12:13:26 2005  Link Down [Port 1]
3)  Wed Apr 13 11:58:31 2005  Login [admin]
4)  Wed Apr 13 11:19:45 2005  Login [admin]
5)  Wed Apr 13 11:19:37 2005  Logout [admin]
```

clear

Syntax:
clear
Description:
Clears the log data.
Argument:
None.
Possible value:
None.
Example:
065-7840(log)# clear

upload

Syntax:
Upload
Description:
Uploads log data through TFTP.
Argument:
None.
Possible value:
None.
Example:
065-7840(log)# upload

enable auto-upload

Syntax:
enable auto-upload
Description:
Enables the auto-upload function.
Argument:
None.
Possible value:
None.
Example:
065-7840(log)# enable auto-upload

disable auto-upload

Syntax:
disable auto-upload
Description:
Disables the auto-upload function.
Argument:
None.
Possible value:
None.
Example:
065-7840(log)# disable auto-upload

■ firmware

set upgrade-path

Syntax:
set upgrade-path <filepath>
Description:
Sets up the file path to the image file that will be upgraded.
Argument:
<filepath>: upgrade file path
Possible value:
<filepath>: upgrade file path
Example:
065-7840(firmware)# set upgrade-path gs2124_v0.96.bin.gz

upgrade

Syntax:
upgrade
Description:
Initiates the upgrade function.
Argument:
None
Possible value:
None
Example:
065-7840(firmware)# upgrade
Upgrading firmware ...

show

Syntax:
show
Description:
Displays the IP address of the TFTP server and the upgrade path information.
Argument:
None
Possible value:
None
Example:
065-7840(firmware)# show
TFTP Server IP Address: 192.168.3.111
Path and Filename : gs2124_v0.96.bin.gz

■ config-file

set export-path

Syntax:
set export-path <filepath>
Description:
Sets up the filepath and filename to which the configuration file will be exported.
Argument:
<filepath>:filepath and filename
Possible value:
<filepath>:filepath and filename
Example:
065-7840(config-file)# set export-path log/21511.txt

set import-path

Syntax:
set import-path <filepath>
Description:
Sets up the filepath and filename from which the configuration file will be imported.
Argument:
<filepath>:filepath 和 filename
Possible value:
<filepath>:filepath 和 filename
Example:
065-7840(config-file)# set import-path log/21511.txt

e*xport start*

Syntax:
export start
Description:
Initiates the export of the configuration file.
Argument:
None
Possible value:
None
Example:
065-7840(config-file)# export start
Export successful.

e*xport user-conf*

Syntax:
export user-conf
Description:
Initiates the export of the user configuration file.
Argument:
None
Possible value:
None
Example:
065-7840(config-file)# export user-conf
Export successful.

import start

Syntax:
import start
Description:
Initiates the import of the configuration file.
Argument:
None
Possible value:
None
Example:
065-7840(config-file)# import start
Import successful.

import user-conf

Syntax:
import user-conf
Description:
Initiates the import of the user configuration file.
Argument:
None
Possible value:
None
Example:
065-7840(config-file)# import user-conf
Import successful.

show

Syntax:
show
Description:
Displays the import and export file location information (filepath, file name, and TFTP Server IP address).
Argument:
None
Possible value:
None
Example:
065-7840(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: nmap/123.ts
Import Path and Filename: user123.txt

■ TFTP

set server

Syntax:
set server <ip>
Description:
Sets up the IP address of the TFTP server.
Argument:
<ip>: tftp server ip
Possible value:
<ip>: tftp server ip
Example:
065-7840(tftp)# set server 192.168.3.111

show

Syntax:
show
Description:
Displays the IP address information of the TFTP server.
Argument:
None
Possible value:
None
Example:
065-7840(tftp)# show
TFTP Server : 192.168.3.111

■ hostname

hostname

Syntax:
hotsname <range> <data_rate>
Description:
Sets up the hostname of the switch.
Argument:
<name>: hostname, max 128 characters.
Possible value:
<name>: hostname, max 128 characters.
Example:
065-7840# hostname Company

Company#

■ autologout

autologout

Syntax:
autologout <time>
Description:
Sets up the auto-logout timer.
Argument:
<time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.
Possible value:
<time>: 0,1-3600
Example:
065-7840# autologout 3600
Set autologout time to 3600 seconds

■ reboot

reboot

Syntax:
reboot
Description:
Initiates a reboot of the system.
Argument:
None
Possible value:
None
Example:
065-7840# reboot

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.
   - ✓ The network interface of Computer C may have failed. Please check the link/activity status of Computer C on the LED indicator of Computer C's network interface as well as that of the switch. Try another network device on this connection.
   - ✓ The network configuration of Computer C may be incorrect. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.
   - ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that Managed Switch.
   - ✓ Please check the uplink setup of the Managed Switch to verify that the uplink function is enabled.

3. The console interface cannot appear on the console port connection.
   - ✓ The COM port default parameters are [Baud Rate: 57600, Data Bits: 8, Parity Bits: None, Stop Bit: A, Flow Control: None]. Please check the COM port properties in the terminal emulator program. If the parameters are different, please set the COM configuration to the new setting.
   - ✓ Check that the RS-232 cable is securely connected on the console port of the Managed Switch and the COM port of the PC.
   - ✓ Check if the COM of the PC is enabled.

4. How is the Managed Switch configured?
   - ✓ "HyperTerminal" is the terminal emulator program in Win95/98/NT/XP. Users can also use any other terminal programs in Linux/Unix to configure the Managed Switch. Please refer to the user's guide of that terminal program. Please note that the COM port parameters (baud rate/ data bits/ parity bits/ flow control) must be the same as the setting of the console port of the Managed Switch.

Appendix A
Technical Specifications

Features

- 22 (10/100/1000 Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE 802.3, 802.3u, 802.3z and 802.3ab standards.
- 2 Gigabit TP/SFP fiber ports are dual media ports with an auto-detection function.
- Non-blocking store-and-forward shared-memory, Web-Smart switched.
- Supports auto-negotiation for configuring speed and duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any of the ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Auto-aging with programmable inter-age time.
- Supports port sniffer functionality via the Port Mirroring feature
- Programmable maximum Ethernet frame length ranging from 1518 to 9216 bytes jumbo frame.
- Supports port-based VLAN and 802.1Q tag-based VLAN.
- Efficient self-learning and address recognition mechanism enables wire speed forwarding rates.
- Web-based management provides the ability to completely manage the switch from any web browser.
- SNMP/Telnet interface delivers complete in-band management.
- Supports IEEE 802.1d Spanning Tree Protocol.
- Supports IEEE 802.1w Rapid Spanning Tree Protocol.
- Supports IEEE 802.1x port-based network access control.
- Supports IEEE 802.1v protocol-based VLAN classification.
- Supports IP Multicasting to implement the IGMP Snooping function.
- Supports 802.1p Prioritization of Service (a.k.a. Class of Service) with 2-level priority queuing.
- Supports 802.3ad port trunking with flexible load distribution and automatic failover functionality.
- Supports ingress port security mode for VLAN Tagged and Untagged frame processing.
- Supports SNMP MIB2 and RMON sampling with sampled packet error indication.

Hardware Specifications

- **Standard Compliance:**
  IEEE 802.3 10BaseT
  IEEE 802.3u 100BaseTX
  IEEE 802.3ab 1000BaseT
  IEEE 802.3z 1000BaseSX/LX
  IEEE 802.1p Priority (Quality of Service [QoS])
  IEEE 802.1D/802.1w/802.1s Spanning Tree & Rapid Spanning Tree Protocols
  IEEE 802.1Q Tagged VLAN with "Q-in-Q" support
  IEEE 802.3x Flow Control
  IEEE 802.3ad Link Aggregation
  IEEE 802.1x Access Control

- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000 Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 24
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	23,24(Optional)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	23,24(Optional)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	23,24(Optional)

*Port 23, 24 are TP/SFP fiber dual media ports with auto-detection function
*Optional SFP module supports LC or BiDi LC transceiver

- **Transmission Mode:** 10/100Mbps supports full or half duplex
  1000 Mbps supports full duplex only

- **Transmission Speed:** 10/100/1000 Mbps for TP
  1000 Mbps for Fiber

- **Full Forwarding/Filtering Packet Rate:**

Forwarding Rate	Speed
1,488,000 pps	1000 Mbps
148,800 pps	100 Mbps
14,880 pps	10 Mbps

(pps = packets per second)

- **MAC Address and Self-learning:** 8K MAC addresses
  4K VLAN table entries

- **Buffer Memory:** Embedded 400 KB frame buffer

- **Flow Control:** IEEE 802.3x compliant for full duplex
  Backpressure flow control for half duplex

- **Cable Type and Maximum Length:**

TP	Cat. 5e or better UTP cable, up to 100 m
1000BaseSX	Up to 220/275/500/550m, which depends on Multimode Fiber type
1000BaseLX	Single-Mode Fiber, up to10/30/50 km
1000BaseLX WDM (BiDi)	Single-Mode Single Fiber, up to 20 km

- **Diagnostic LEDs:**
  System LEDs : Power, CPU
  Per Port LEDs:
  10/100/1000 Mbps TP Ports 1 to 24: LINK/ACT, 10/100/1000 Mbps
  1000 Mbps SFP Fiber Ports 23 & 24: SFP (LINK/ACT)

- **Power Requirement:**
  Voltage: 100~240 Volts AC
  Frequency: 50~60 Hz
  Power Consumption: 30 Watts

- **Ambient Temperature:** 32° to 122°F [0° to 50°C]
- **Humidity:** 5% to 90%
- **Dimensions:** 1.73 in.(H) × 17.4 in.(W) × 8.23 in.(D) [44 × 442 × 209 mm]
- **Emissions:** Complies with FCC Part 15, Class A & CE Mark Approval

Management Software Specifications

System Configuration	Auto-negotiation support on 10/100/1000 Base-TX ports, Web browser or console interface can set transmission speed (10/100/1000 Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
Management Agent	SNMP support; MIB II, Bridge MIB, RMON MIB
Spanning Tree Algorithm	IEEE 802.1D
VLAN Function	Port-Base / 802.1Q-Tagged, allows up to 256 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
IGMP	IP Multicast Filtering by passively snooping on the IGMP Query.
Bandwidth Control	Supports by-port Egress/Ingress rate control
Quality of Service (QoS)	Referred as Class of Service (CoS) by the IEEE 802.1p standard Four queues per port Packet transmission schedule using Weighted Round Robin (WRR) User-defined weight Classification of packet priority can be based on either a VLAN tag on packet or a user-defined port priority.
Port Security	Limits the number of MAC addresses learned per Port; static MAC addresses stay in the filtering table.
Internetworking Protocol	Bridging : 802.1D Spanning Tree IP Multicast: IGMP Snooping IP Multicast Packet Filtering Maximum of 256 active VLANs and IP multicast sessions
Network Management	One RS-232 port as local control console Telnet remote control console SNMP agent : MIB-2 (RFC 1213) Bridge MIB (RFC 1493) RMON MIB (RFC 1757)-statistics VLAN MIB (802.1Q) Web browser support based on HTTP Server and CGI parser TFTP software upgrade capability.

Note: All specifications are subject to change without notice.

Appendix B
Null Modem Cable Specifications

The DB-9 cable is used for connecting a terminal or terminal emulator to the Managed Switch's RS-232 port to access the command line interface.

The table below shows the pin assignments for the DB-9 cable.

Function	Mnemonic	Pin
Carrier	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

9 Pin Null Modem Cable